Manuscript submitted to *Security and Safety*, For Peer Review Only, Vol. x, xxxxxxx (2023)
https://doi.org/10.1051/sands/xxxxxxx
sands.edpsciences.org

Research Article OPEN ACCESS

Section Category

Distributed Secure State Estimation for CPSs Based on Side Information

Zheyi Zhao[1], Xuqiang Lei[2*], and Huian Yan[3]

[1] *School of Sciences, Liaoning Technical University, Fuxin 123000, China*
[2] *School of Mathematics, Southeast University, Nanjing 211189, China*
[3] *School of electrical and control engineering, Liaoning Technical University, Nanjing 211189, China*

Received: 15 November 2025 / Revised: 18 January 2026 / Accepted: xx xxxxx 2025 / Published online: xx xxxxx 2025

Abstract The distributed nature of cyber-physical systems exposes them to severe security threats, where attackers can compromise measurement data through sensor networks, leading to significant physical consequences. Existing research on secure state estimation primarily focuses on optimizing efficiency and improving estimation accuracy, often relying on the strong assumption that the number of compromised sensors does not exceed half of the total, which limits system resilience. To overcome this limitation, this paper proposes a distributed secure state estimation algorithm incorporating side prior information. By integrating side information with a distributed optimization framework, a more resilient secure estimation model is constructed. Theoretical analysis proves the convergence of the algorithm under the $(\Psi, 2l)$-observability condition. Numerical simulations demonstrate that the proposed algorithm effectively enhances the system's tolerance to sparse sensor attacks, enabling accurate state estimation even when more than half of the sensor channels are compromised.

Keywords Cyber-Physical System, Secure State Estimation, Distributed Algorithm, Side Prior Information, System Resilience

Citation Zheyi Zhao, Xuqiang Lei and Huian Yan. Distributed Secure State Estimation for CPSs Based on Side Information. Security and Safety 2023; **x**: xxxxxxx. https://doi.org/10.1051/sands/xxxxxxx

1 Introduction

Cyber-physical system(CPSs), as deep integrations of physical hardware and network software, plays crucial roles in numerous fields through the tight coordination of physical processes, computational resources, and communication capabilities. However, their distributed nature also introduces significant security vulnerabilities [1, 2]. Attackers can infiltrate sensor networks via worms, false data injection, etc., to tamper with measurement data [3]. Given the deep coupling between the cyber and physical realms, attacks on cyber-physical systems can lead to severe physical consequences, as evidenced by typical cases such as the Stuxnet incident [4], the Marucchi Water intrusion [5], and the Ukrainian grid hack [6], underscoring the importance and urgency of research on System Security Technology.

To counter various attacks, researchers have proposed multiple security defense strategies. For instance, [7] proposed a secure control method for achieving pinning synchronization in cyber-physical systems under malicious node attacks. [8] designed a fixed-time observer-based attack isolation algorithm to enhance the resilience of multi-agent systems against non-collusive and undetectable collusive link attacks. [9] established an isolation mechanism for collaborative false data injection and stealthy attacks in interconnected systems under graph-theoretic conditions. Concurrently, the problem of secure state

* Corresponding author (email: xq-lei@seu.edu.cn)

estimation(SSE) under sensor attacks has garnered. Research in this area often transforms the state estimation problem into an error correction problem, solved by compressed sensing techniques [10]. Among specific implementation methods, static batch processing algorithms are a common category, whose core idea involves collecting sensor observations over T time steps and formulating the SSE problem as a static optimization problem. References [11–13] proposed effective optimization algorithms to search for possible attack combinations and identify anomalous data. However, they were all constrained by the minimization of non-convex l_0-constrained problems. To address this, [14–16] relaxed it into convex $\ell_1/\ell_r(r>1)$ optimization problems for solution. To further improve estimation efficiency, some studies employ greedy algorithms and geometric algorithms, such as [17–20], which utilized gradient descent and projection algorithms to enhance computational efficiency and reduce complexity.

However, the aforementioned studies primarily focus on improving optimization efficiency and reducing estimation errors, without sufficiently addressing the enhancement of system resilience. Most of these works are based on deterministic attack assumptions: namely, the number of attacked sensors does not exceed half of the total number of sensors, consistent with the attack model set in [16]. To increase the upper limit of tolerable sensor attacks in cyber-physical systems, some research has begun to explore the introduction of prior information to relax system observability conditions. For example, [21] introduced two types of prior information to relax the necessary conditions for system observability, and provided new insights for enhancing the resilience of SSE algorithms. [22] proposed a candidate set construction algorithm incorporating side information to detect more attacks. [23] utilized prior information to reduce redundancy requirements for measurement and communication networks. These studies indicate the significant potential of using prior information to enhance system resilience against sparse sensor attacks. Nevertheless, to the best of our knowledge, no effective breakthroughs have been achieved in enhancing resilience based on side information within distributed SSE frameworks. Therefore, this paper attempts to combine side information with distributed SSE algorithms to construct a more robust secure estimation framework.

The main contributions of this paper can be summarized as follows. First, we propose a distributed SSE algorithm enhanced by side information to improve resilience against sparse sensor attacks, building upon the work of [20]. Second, in contrast to the centralized SSE frameworks leveraging prior information [21], our work extends this research to a distributed setting. Third, by integrating side information into the estimation process, we generalize the method relied solely on sparse prior information in [23], thereby substantially relaxing the constraints on prior information.

The structure of this paper is organized as follows. Section 2 elaborates the basic graph theory, problem model and reviews research on enhancing anti-attacked capability in CPS systems based on side prior information. In Section 3, a novel distributed SSE scheme is proposed by utilizing side prior information. Section 4 provides evidence for the performance of the distributed SSE algorithm. Section 6 validates the algorithm effectiveness through numerical simulations. Finally, conclusions are presented in Section 7.

Notation: Let $\mathbb{R}^n$ denote the n-dimensional Euclidean space, and $\mathbb{N}^+$ denotes the set of natural numbers excluding 0. The symbol $\mathbf{0}$ represents an n-dimensional column vector with all elements being 0. The symbol $\mathcal{N}$ denotes the index set $\{1,2,\ldots,n\}$, and $\mathcal{M}$ denotes the index set $\{1,2,\ldots,m\}$. For $x\in\mathbb{R}^n$, x_p denotes the p-th element of x, where $p\in\mathcal{N}$; $\mathrm{supp}(x)$ denotes the support set of x; $\|x\|_g$ denotes its ℓ_g-norm, where $g\geq 1$. In particular, $\|x\|_0=|\mathrm{supp}(x)|$. If $\|x\|_0\leq l$, then x is said to be l-sparse.

For a matrix $A\in\mathbb{R}^{m\times n}$ and an index subset $\Gamma\subseteq\mathcal{M}$, A_Γ denotes the matrix consisting only of the rows index by Γ, and $A_{\overline{\Gamma}}$ denotes the matrix remaining after removing all rows index by Γ. Given a natural number $g\geq 1$, define the ℓ_1/ℓ_g mixed norm of A as $\|A\|_{1/g}\triangleq\sum_{p=1}^{m}\|A_p\|_g$. In particular, the ℓ_0/ℓ_g mixed norm of A is $\|A\|_{0/g}\triangleq\sum_{p=1}^{m}\mathrm{II}(\|A_p\|_g)$, where $\mathrm{II}(z)=0$ if $z=0$, and 1 otherwise. If $\|A\|_{0/g}\leq l$, then A is said to be l-sparse.

2 Preliminaries

2.1 Graph Theory

This subsection presents fundamental concepts in graph theory that underpin the distributed framework discussed in this paper. Consider a network of sensors or agents, whose communication topology is modeled as an undirected graph $\mathcal{G}=(\mathcal{V},\mathcal{E})$. Here, $\mathcal{V}=\{1,2,\ldots,v\}$ is the set of nodes, and $\mathcal{E}\subseteq\mathcal{V}\times\mathcal{V}$ is

the set of edges. The interaction between neighboring agents i and j is characterized by a non-negative communication weight $a_{ij} > 0$ if $(i, j) \in \mathcal{E}$, and $a_{ij} = 0$ otherwise. These weights together form the adjacency matrix $\mathcal{A} = [a_{ij}] \in \mathbb{R}^{n\times n}$ of the graph $\mathcal{G}$. The communication network between sensor clusters can be represented by an undirected connected graph $\mathcal{G}$, meaning a path exists between any two distinct nodes.

2.2 System Formulation

Consider a discrete linear time-invariant autonomous system monitored in a distributed manner by p sensor clusters, each producing a varying number of measurements, as follows:

$$\begin{cases} x(k+1) = Ax(k), \\ y_i(k) = C_i x(k) + a_i(k), \end{cases} \tag{1}$$

where the system state $x(k) \in \mathbb{R}^n$, the system output $y_i(k) \in \mathbb{R}^{q_i}$, which may be compromised by malicious attack $a_i(k) \in \mathbb{R}^{q_i}$, $k \in \mathbb{N}$ represents the k-th sampling time step, $i \in \{1, 2, \ldots, p\}$ represents the index of the sensor cluster, q_i represents the output dimension of sensor cluster i, and matrices A, C_i have appropriate dimensions.

Additionally, consider that the operator possesses the following side information for system (1):

$$\Psi x = \mathbf{0}. \tag{2}$$

Assumption 1. Ψ has full row rank, and Ψ is known by all sensor clusters.

Remark 2. The full row rank condition on Ψ is both practical and mild. Physically, each row of $\Psi x = \mathbf{0}$ typically represents an independent piece of side information. If Ψ is deficient row rank, one can always extract a maximal set of independent rows to form a new matrix satisfying this assumption without altering the constraint set.

Remark 3. The side information $\Psi x = \mathbf{0}$ stems from practical physical laws, operational constraints, or prior knowledge about the system. For example, Physical laws: In power systems, Kirchhoff's laws impose linear relationships among state variables. Geometric constraints: In robotic or formation control, distances or relative positions between agents may satisfy known linear equations. Mass/energy balance: In chemical or hydraulic networks, conservation laws under steady-state assumptions provide linear constraints on state variables.

To clearly articulate the SSE problem under sparse attacks, we begin by revisiting the problem of SSE within centralized system, and then extend the concept to a distributed framework. Performing centralized augmentation for system (1), for each time step k, define:

$$C = [C_1^\top, \ldots, C_p^\top]^\top,$$
$$y(k) = [y_1^\top(k), \ldots, y_p^\top(k)]^\top,$$
$$a(k) = [a_1^\top(k), \ldots, a_p^\top(k)]^\top.$$

Thus, we have:

$$y(k) = Cx(k) + a(k).$$

Further collecting and augmenting the system outputs from time 0 to $\tau - 1$ (a total of τ time steps) yields the following form:

$$Y = \Phi(x) + Y_a, \tag{3}$$

where

$$Y = [y(0), y(1), \ldots, y(\tau-1)],$$
$$\Phi(x) = [Cx, CAx, \ldots, CA^{\tau-1}x],$$
$$Y_a = [a(0), a(1), \ldots, a(\tau-1)].$$

Similarly, define the function corresponding to each sensor cluster based on $\Phi(x)$:

$$\Phi_i(x) = [C_i x, \ldots, C_i A^{\tau-1} x].$$

Analogously, one has $Y_i = \Phi_i(x) + Y_{ai}$ with $Y_i = [y_i(0), ..., y_i(\tau-1)]$ and $Y_{ai} = [a_i(0), \ldots, a_i(\tau-1)]$. Furthermore, the following two assumptions are made.

Assumption 4. In system (1), matrix A and the augment matrix C is observable.

It is critical to note that this assumption is fundamental to the design of a distributed estimator, even in a non-adversarial setting. Nevertheless, we emphasize that the pair (A, C_i) need not be observable for any individual sensor cluster $i \in 1, 2, \ldots, p$. Additionally, we make the following assumption regarding the malicious adversary.

Assumption 5. The malicious attacker can compromise at most l sensor channels, i.e., for any positive integer k, $|\mathrm{supp}(a(k))| \leq l$. Moreover, the attack support set is time-invariant, meaning that $\mathrm{supp}(a(k))$ remains constant over time.

Remark 6. The time-invariance of the attack support set in Assumption 5 is justified by practical considerations. Attackers often have limited energy and resources, so they tend to persist with successfully compromised vulnerabilities rather than frequently shifting attack positions. Changing attack positions would require additional effort to exploit new vulnerabilities, which may be inefficient and risky. Furthermore, in many cyber-physical systems, attacks like false data injection or sensor tampering are often sustained on fixed channels to maintain stealth and effectiveness. Thus, this assumption aligns with common attack behaviors in real-world scenarios.

Remark 7. The malicious attacker is omniscient, meaning the attacker has full knowledge of system (1). In addition, it is assumed that collusion among all malicious sensor clusters is permitted.

2.3 Centralized Optimization Problem Formulation

For system (1), its observability matrix is:

$$O = [C^\top, \ldots, (CA^{n-1})^\top]^\top.$$

Correspondingly, $O_{\overline{\Gamma}}$ denotes the observability matrix constructed for $(A, C_{\overline{\Gamma}})$, i.e.,

$$O_{\overline{\Gamma}} = [C_{\overline{\Gamma}}^\top, \ldots, (C_{\overline{\Gamma}} A^{n-1})^\top]^\top.$$

This leads to the definition of a specific system observability as follows.

Definition 8. For system (1) and a positive integer l, if for every $\Gamma \subseteq \{1, \ldots, p\}$ with $|\Gamma| \leq l$, it holds that $\ker(O_{\overline{\Gamma}}) \cap \ker(\Psi) = \{0\}$, then system (1) is said to be (Ψ, l)-observable.

Proposition 9. *For l-sparse attacks, system (1) can successfully estimate the initial state under the side information (2) if and only if system (1) is $(\Psi, 2l)$-observable.*

Proof. For the proof of sufficiency, assume the system (1) is $(\Psi, 2l)$-observable, yet the initial state and attack sequences fail to be estimate. For the sake of contradiction, suppose there exist two distinct initial states x_1, x_2 with $x_1, x_2 \in \ker(\Psi)$ and two disparate sets of attack vectors a', a'' with $\mathrm{supp}(a') \subseteq \Gamma'$ and $\mathrm{supp}(a'') \subseteq \Gamma''$ satisfying $|\Gamma'| \leq l$ and $|\Gamma''| \leq l$, that generate the same output sequence $y(k) = CA^{k-1}x_1 + a'(k) = CA^{k-1}x_2 + a''(k)$. Then,

$$CA^{k-1}(x'' - x') = a'(k) - a''(k).$$

Since $|\Gamma'| \leq l$ and $|\Gamma''| \leq l$, then $x'' - x' \in \ker(O_{\overline{\Gamma' \cup \Gamma''}})$, where $|\Gamma' \cup \Gamma''| \leq 2l$. It is obvious that $x'' - x' \in \ker(\Psi)$, then it leads to a contradiction that a nonzero vector $x'' - x' \in \ker(O_{\overline{\Gamma}}) \cap \ker(\Psi)$.

For the necessity, suppose that any initial state consistent with the side information and any sparse attacks can be uniquely estimated, yet the system is not $(\Psi, 2l)$-observable. It then follows that for some index set Γ with $|\Gamma| \leq 2l$, a nonzero vector x exists such that $x \in \ker(O_{\overline{\Gamma}}) \cap \ker(\Psi)$.

For $a(k) = CA^{k-1}x$, since $x \in \ker(O_{\overline{\Gamma}})$, then $|\operatorname{supp}(a(k))| \leq 2l$. Thus, there are two index set $|\Gamma'| \leq l$ and $|\Gamma''| \leq l$, satisfy that $\Gamma' \cup \Gamma'' = \Gamma$ and $\Gamma' \cap \Gamma'' = \emptyset$. Based on Γ' and Γ'', define $a'(k)$ by changing all the components in $a(k)$ that do not belong to Γ' to 0 and $a''(k)$ by changing all the components in $a(k)$ that do not belong to Γ'' to 0. In other word:

$$a'_i(k) = \begin{cases} a_i, & \text{if } i \in \Gamma' \\ 0, & \text{otherwise.} \end{cases}, \quad a''_i = \begin{cases} a_i, & \text{if } i \in \Gamma'' \\ 0, & \text{otherwise.} \end{cases}$$

Clearly, $\operatorname{supp}(a'(k)) = \Gamma'$ and $\operatorname{supp}(a''(k)) = \Gamma''$.

Since $x \in \ker(\Psi)$, there are two distinct initial states x_1, x_2 with $x_2 - x_1 = x$. Thus,

$$CA^{k-1}(x_2 - x_1) = CA^{k-1}x = a(k) = a'(k) + a''(k),$$

which applies that

$$CA^{k-1}x_2 - a''(k) = CA^{k-1}x_1 + a'(k).$$

Since $\operatorname{supp}(-a''(k)) = \operatorname{supp}(a''(k))$, it means that two different initial state can produce the same output. Thus, it is impossible to successfully estimate the initial state, which implies a contradiction. □

The preceding analysis establishes a necessary and sufficient condition for uniquely estimating the initial state of system (1) subject to the side information (2). Then, to securely and accurately estimate the true state of system (1), the following centralized nonconvex optimization problem is formulated:

$$\begin{aligned} P_0 : \arg\min_{\hat{x} \in \mathbb{R}^n} \quad & \sum_{i=1}^{p} \|Y_i - \Phi_i(\hat{x})\|_{0/g} \\ \text{s.t. } & \Psi\hat{x} = \mathbf{0}. \end{aligned} \tag{4}$$

Naturally, for the sake of convenience in solving, the following convex optimization problem is constructed:

$$\begin{aligned} P_1 : \arg\min_{\hat{x} \in \mathbb{R}^n} \quad & \sum_{i=1}^{p} \|Y_i - \Phi_i(\hat{x})\|_{1/g} \\ \text{s.t. } & \Psi\hat{x} = \mathbf{0}, \end{aligned} \tag{5}$$

where g is a positive integer greater than 1.

Lemma 10. *[21] The optimal solutions given by P_0 and P_1 are identical if and only if for every $\Gamma \subseteq \{1, \ldots, p\}$ with $|\Gamma| \leq l$ and every $x \in \ker(\Psi)$, the following holds:*

$$\sum_{i \in \Gamma} \|\Phi_i(x)\|_{1/g} < \sum_{i \in \overline{\Gamma}} \|\Phi_i(x)\|_{1/g}. \tag{6}$$

Remark 11. From lemma 10, it can be obtained that there exist $p \in (0, 1)$, such that

$$p \sum_{i \in \overline{\Gamma}} \|\Phi_i(z)\|_{1/1} > \sum_{i \in \Gamma} \|\Phi_i(z)\|_{1/1}.$$

3 Distributed Algorithm Formulation

Proposition 9 provides the necessary and sufficient condition for the system to successfully estimate the initial state and transforms the problem into a centralized convex optimization model. This section describes the process of converting this centralized convex optimization problem into a distributed form.

First, a projection operator is introduced. For a set G, $P_G(x)$ is the projection vector obtained by projecting the current vector x onto G, i.e.,

$$P_G(x) = \arg\min_{\hat{x}\in G} \quad \|\hat{x} - x\|_2.$$

Proposition 12. *If the matrix Ψ is full row rank, then*

$$P_{\ker(\Psi)}(x) = x - \Psi^\top(\Psi\Psi^\top)^{-1}\Psi x. \tag{7}$$

Proof. The projection operator $P_{\ker(\Psi)}(x)$ is defined as the solution to the following optimization problem:

$$\begin{aligned} \min_{z} \quad & \|z - x\|_2^2 \\ \text{s.t.} \quad & \Psi z = \mathbf{0}. \end{aligned} \tag{8}$$

Construct the Lagrangian function:

$$L(z, \lambda) = \|z - x\|_2^2 + \lambda^\top \Psi z,$$

where $\lambda \in \mathbb{R}^m$ is the Lagrange multiplier.

Taking the gradient with respect to z and setting it to zero:

$$\nabla_z L = 2(z - x) + \Psi^\top \lambda = \mathbf{0} \quad \Rightarrow \quad z = x - \frac{1}{2}\Psi^\top \lambda.$$

Substituting into the constraint $\Psi z = \mathbf{0}$:

$$\Psi\left(x - \frac{1}{2}\Psi^\top \lambda\right) = \mathbf{0} \quad \Rightarrow \quad \Psi x = \frac{1}{2}\Psi\Psi^\top \lambda.$$

Solving for λ:

$$\lambda = 2(\Psi\Psi^\top)^{-1}\Psi x.$$

Substituting back into the expression for z:

$$z = x - \frac{1}{2}\Psi^\top \left[2(\Psi\Psi^\top)^{-1}\Psi x\right] = x - \Psi^\top(\Psi\Psi^\top)^{-1}\Psi x.$$

Therefore, one has

$$P_{\ker(\Psi)}(x) = x - \Psi^\top(\Psi\Psi^\top)^{-1}\Psi x.$$

□

Relying on the projection operator, we next present a distributed SSE algorithm incorporating side information. Define the distributed objective function as

$$f_i(x) = \|\Phi_i(x) - Y_i\|_{1/1}. \tag{9}$$

Then, the distributed algorithm can be expressed as:

$$\begin{cases} v_i^t = \sum_{j=1}^p w_{ij}\hat{x}_j^t, \\ \sigma_i^t = v_i^t - \alpha^t d_i^t(v_i^t), \\ \hat{x}_i^{t+1} = P_{\ker(\Psi)}(\sigma_i^t), \end{cases} \tag{10}$$

where w_{ij} w_{ij} is a parameter to be designed subsequently corresponding to the computational weight that sensor cluster i assigns to cluster j , $\hat{x}_i^t$ represents the estimation of the initial state by the i-th sensor

cluster at iteration $t \in \mathbb{N}^+$, starting from an arbitrary initial guess $\hat{x}_i^0$. α^t is a finite step size. $d_i^t(v_i^t)$ is a subgradient of the function $f_i(x)$ at $x = v_i^t$. For a vector $x \in \mathbb{R}^n$, based on the definition of $f_i(x)$, the subgradient is:

$$d_i(x) = \nabla f_i(x) = \sum_{l=1}^{q_i} \sum_{\iota=1}^{\tau} \operatorname{sgn}([O_{i,l}]_\iota x - [Y_{i,l}^\top]_\iota)[O_{i,l}]_\iota^\top, \tag{11}$$

where sgn is the sign function with $\operatorname{sgn}(0) = 0$, $O_{i,l} \in \mathbb{R}^{\tau \times n}$ is the observability matrix for the l-th output of the i-th sensor cluster, specifically:

$$O_{i,l} = [[C_i]_l^\top, \ldots, ([C_i]_l A^{\tau-1})^\top]^\top \in \mathbb{R}^{\tau \times n}.$$

Furthermore, $[O_{i,l}]_\iota \in \mathbb{R}^{1 \times n}$ is the ι-th row of matrix $O_{i,l}$.

Remark 13. The function $f_i(x) = \|\Phi_i(x) - Y_i\|_{1/1}$ is convex as it is a sum of ℓ_1 norms of affine functions. For a convex function $h(x) = \|Ax - b\|_1$, its subgradient at x is given by $\partial h(x) = A^\top \operatorname{sgn}(Ax - b)$, where $\operatorname{sgn}(\cdot)$ applied to a vector returns the vector of signs, with the convention:

$$\operatorname{sgn}(z) = \begin{cases} 1, & \text{if } z > 0, \\ [-1, 1], & \text{if } z = 0, \\ -1, & \text{if } z < 0. \end{cases}$$

When $[O_{i,l}]_\iota x - [Y_{i,l}^\top]_\iota = 0$, any value in $[-1, 1]$ is a valid subgradient component. In our algorithm, we adopt the specific choice of $\operatorname{sgn}(0) = 0$, which yields a particular subgradient $d_i(x)$ defined in (11). This choice satisfies the subgradient inequality:

$$f_i(y) \geq f_i(x) + d_i(x)^\top (y - x), \quad \forall y \in \mathbb{R}^n,$$

and ensures boundedness of $d_i(x)$.

Similarly, $Y_{i,l} \in \mathbb{R}^{1 \times \tau}$ is the augmented form of the l-th output of the i-th sensor cluster, specifically:

$$Y_{i,l} = [[y_i(0)]_l, \ldots, [y_i(\tau - 1)]_l] \in \mathbb{R}^{1 \times \tau}.$$

And $[Y_{i,l}^\top]_\iota \in \mathbb{R}$ is the ι-th value of $Y_{i,l}$.

Finally, the step size a^t and the computational weight w_{ij} are designed as follows.

Considering that the step size satisfies the following properties:

$$\lim_{t \to \infty} \alpha^t = 0, \quad \sum_{t=1}^{\infty} (\alpha^t)^2 < \infty. \tag{12}$$

Regarding the weights, a feasible approach could be designed as follows:

$$w_{ij} = \frac{a_{ij}}{\sum_{j=1}^{p} a_{ij}}. \tag{13}$$

Remark 14. In this paper, the communication topology is an undirected graph, thus $w_{ij} = w_{ji}$, and $\sum_{i=1}^{p} w_{ij} = \sum_{j=1}^{p} w_{ij} = 1$.

4 Algorithm Feasibility Proof

In the previous section, the local estimation protocol (10) was designed as the distributed subgradient SSE algorithm. This section proves the effectiveness of this distributed subgradient SSE algorithm. Prior to this, the following two lemmas can be introduced to facilitate the analysis of the main results in this paper.

Lemma 15. *[24] For $\forall z \in \ker(\Psi)$ and $\forall t \geq 0$, if the weights are given by (13), then*

$$\sum_{i=1}^{p} \|\hat{x}_i^{t+1} - z\|_2^2 \leq \sum_{i=1}^{p} \|\hat{x}_i^t - z\|_2^2 + (\alpha^t)^2 \|d_i(v_i^t)\|_2^2 - 2\alpha^t \sum_{i=1}^{p} (f_i(v_i^t) - f_i(z)) - \sum_{i=1}^{p} \|\eta_i^t\|_2^2,$$

where $\eta_i^t = \hat{x}_i^{t+1} - \sigma_i^t$.

Define the iteration $\xi^{t+1} = \xi^t - \frac{\alpha^t}{p}\sum_{i=1}^p d_i(v_i^t) + \frac{1}{p}\sum_{i=1}^p \eta_i^t$, with $\xi^0 = \frac{1}{p}\sum_{i=1}^p \hat{x}_i^0$.

Lemma 16. *[24] If the weights are given by (13), then*
(1) If $\lim_{t\to\infty}\alpha^t = 0$, then for $\forall i$, $\lim_{t\to\infty}\|\hat{x}_i^t - \xi^t\|_2 = 0$.
(2) If $\sum_{t=1}^{\infty}(\alpha^t)^2 < \infty$, then for $\forall i$, $\sum_{t=1}^{\infty}\alpha^t\|\hat{x}_i^t - \xi^t\|_2 < \infty$.

Based on the above two lemmas, we can prove the feasibility of the distributed subgradient SSE algorithm.

Theorem 17. *If Assumptions 4-5 hold, system (1) is (Ψ, l)-observable, and (6) is satisfied. If the weights w_{ij} are given by (13), and the step size α^t satisfies (12), then (10) can successfully estimate the secure initial state, i.e. $\lim_{t\to\infty}\|\hat{x}_i^t - x(0)\|_2 = 0$.*

Proof. From the form of d_i, it is known to be bounded, i.e.,

$$\exists D \in \mathbb{R}, \quad \|d_i(x)\|_2 \le D < \infty.$$

By Lemma 15, the non-negativity of $\|\eta_i^t\|_2^2$, and the fact that $\sum_{i=1}^p f_i(x) = f(x)$, we obtain:

$$\begin{aligned}\sum_{i=1}^p \|\hat{x}_i^{t+1} - z\|_2^2 \le \sum_{i=1}^p \|\hat{x}_i^t - z\|_2^2 + (\alpha^t)^2 pD^2 \\ - 2\alpha^t\sum_{i=1}^p (f_i(v_i^t) - f_i(\xi^t)) - 2\alpha^t(f(\xi^t) - f(z)).\end{aligned} \tag{14}$$

By the definition of the subgradient:

$$|f_i(v_i^t) - f_i(\xi^t)| \le D\|v_i^t - \xi^t\|_2 \le D\sum_{j=1}^p w_{ij}\|\hat{x}_j^t - \xi^t\|_2.$$

Summing the above from $i = 1$ to $i = p$ yields:

$$\begin{aligned}\sum_{i=1}^p |f_i(v_i^t) - f_i(\xi^t)| &\le D\sum_{i=1}^p\sum_{j=1}^p w_{ij}\|\hat{x}_j^t - \xi^t\|_2 \\ &= D\sum_{i=1}^p \|\hat{x}_i^t - \xi^t\|_2,\end{aligned} \tag{15}$$

where the last equation comes from (13).

Substituting (15) into (14) gives:

$$\sum_{i=1}^p \|\hat{x}_i^{t+1} - z\|_2^2 \le \sum_{i=1}^p \|\hat{x}_i^t - z\|_2^2 + (\alpha^t)^2 pD^2 + 2\alpha^t D\sum_{i=1}^p \|\hat{x}_i^t - \xi^t\|_2 - 2\alpha^t(f(\xi^t) - f(z)).$$

Let $z = x(0)$, and sum from $t = 1$ to $t = \tau$, it comes that

$$\begin{aligned}\sum_{i=1}^p \|\hat{x}_i^{\tau+1} - x(0)\|_2^2 + 2\sum_{t=1}^{\tau}\alpha^t(f(\xi^t) - f(x(0))) \\ \le \sum_{i=1}^p \|\hat{x}_i^1 - x(0)\|_2^2 + pD^2\sum_{t=1}^{\tau}(\alpha^t)^2 + 2D\sum_{t=1}^{\tau}\alpha^t\sum_{i=1}^p \|\hat{x}_i^t - \xi^t\|_2.\end{aligned} \tag{16}$$

Since $x(0)$ is the minimizer of $f(x)$, $f(\xi^t) - f(x(0)) \ge 0$, so the second term on the left of inequality (16) can be removed without changing the inequality direction. Thus, the inequality becomes:

$$\sum_{i=1}^p \|\hat{x}_i^{\tau+1} - x(0)\|_2^2 \le \sum_{i=1}^p \|\hat{x}_i^1 - x(0)\|_2^2 + pD^2\sum_{t=1}^{\tau}(\alpha^t)^2 + 2D\sum_{t=1}^{\tau}\alpha^t\sum_{i=1}^p \|\hat{x}_i^t - \xi^t\|_2. \tag{17}$$

By Lemma 16(2), and letting $\tau \to \infty$, the right-hand side of the inequality is bounded, i.e.,

$$\lim_{t\to\infty} \sum_{i=1}^{p} \|\hat{x}_i^t - x(0)\|_2^2 < \infty.$$

Therefore, $\lim_{t\to\infty} \sum_{i=1}^{p} \|\hat{x}_i^t - x(0)\|_2^2$ is bounded.
Reviewing (16), similarly, $\sum_{t=1}^{\infty} \alpha^t (f(\xi^t) - f(x(0)))$ is also bounded.
Since $\sum_{t=1}^{\infty} \alpha^t = \infty$, then it comes that

$$\lim_{t\to\infty} f(\xi^t) - f(x(0)) = 0.$$

Thus,

$$\lim_{t\to\infty} f(\xi^t) = f(x(0)).$$

By the continuity of the function $f(x)$ and $x(0)$ is the minimizer of $f(x)$, we have

$$\lim_{t\to\infty} \xi^t = x(0).$$

By Lemma 16(1), $\lim_{t\to\infty} \|\hat{x}_i^t - \xi^t\|_2 = 0$. Therefore, we can finally conclude: $\lim_{t\to\infty} \|\hat{x}_i^t - x(0)\|_2 = 0$. □

Remark 18. From Theorem 17 that the choice of step size α^t is the key to the success of distributed security state estimation. For the constraint (12), it is easy to verify that $\alpha^t = \frac{1}{t}$ is a feasible solution. Therefore, the distributed estimation protocol (10) is solvable.

Remark 19. In Theorem 17, the condition system (1) is (Ψ, l)-observable is required to be satisfied. This condition directly relates the number of sparse attacks (l) to the success/failure of the secure estimation algorithm. Specifically, let $l_{\max}$ be the maximum integer such that the system is $(\Psi, 2l_{\max})$-observable. Then, the proposed algorithm is guaranteed to recover $x(0)$ when the number of attacked channels does not exceed $l_{\max}$. Conversely, if the number of attacked channels exceeds $l_{\max}$, it is possible that there exist attack patterns that make unique estimation impossible, i.e., the algorithm will fail to converge to the true state.

The proposed distributed algorithm (10) operates in an iterative manner, with each iteration involving local computations at each sensor cluster and communications with its neighbors. We analyze the per-iteration complexity for a single sensor cluster i:

1. Subgradient Computation: Calculating $d_i(v_i^t)$ as in (11) requires evaluating $O(q_i \tau n)$ operations, where q_i is the output dimension of cluster i, τ is the observation window length, and n is the state dimension. This is linear in the problem size and stems from the sum of $q_i\tau$ inner products.
2. Projection Operation: The projection $P_{\ker(\Psi)}(\sigma_i^t)$ in (7), involves computing $\Psi^\top(\Psi\Psi^\top)^{-1}\Psi\sigma_i^t$. The matrix $(\Psi\Psi^\top)^{-1}$ can be precomputed offline, reducing the online complexity to a matrix-vector multiplication of order $O(mn)$, where m is the number of rows in Ψ.
3. Consensus Update: The averaging step $v_i^t = \sum_j w_{ij}\hat{x}_j^t$ requires $O(n|\mathcal{N}_i|)$ operations, where $|\mathcal{N}_i|$ is the number of neighbors of cluster i.

Thus, the overall per-iteration complexity per cluster is $O(q_i\tau n + mn + n|\mathcal{N}_i|)$, which remains polynomial and tractable for practical implementations. The side information constraint $\Psi x = 0$ does not introduce significant additional online burden, as the projection uses a precomputed matrix. The number of iterations required for convergence depends on the step-size schedule α^t and the network connectivity.

5 Secure State Estimation with Measurement Noise

Assumption 20. The measurements are corrupted by a bounded noise. The system model is extended from (1) as:

$$\begin{cases} x(k+1) = Ax(k), \\ y_i(k) = C_i x(k) + a_i(k) + v_i(k), \end{cases} \tag{18}$$

where $v_i(k) \in \mathbb{R}^{q_i}$ is the measurement noise satisfying $\|v_i(k)\|_\infty \leq \bar{v}_i$ for all k and for some known constant $\bar{v}_i$. The attack model in Assumption 5 remains unchanged.

Collecting and augmenting the measurement noise and the attack from time 0 to $\tau-1$ yields the following form:

$$V_i = [v_i(0), v_i(1), \ldots, v_i(\tau-1)],$$
$$Y_{ai} = [a(0), a(1), \ldots, a(\tau-1)].$$

Define $\mathcal{I}_h$ denotes the set of healthy sensors, and $\mathcal{I}_a$ denotes the set of attacked sensors.

Corollary 21 (Robustness under Bounded Noise). *Consider the system under Assumptions 4, 5, and 20. If the conditions of Theorem 17 hold, then the estimates $\hat{x}_i^t$ generated by the distributed algorithm (10) converge to a neighborhood of the true initial state $x(0)$. Furthermore, any limit point $\hat{x}^*$ of the sequence $\{\xi^t\}$ (defined in Lemma 16) satisfies the following error bound:*

$$\|\hat{x}^* - x(0)\|_2 \leq \frac{2\bar{v}\sqrt{\tau p n}}{c(1-p)\sigma_{\min}(\mathcal{O}_\Psi)}, \tag{19}$$

where $\bar{v} = \max_i \bar{v}_i$ is the global noise bound, τ is the observation window length, p is the number of sensor clusters, n is the state dimension, c is the norm equivalence coefficient, p is from remark 11 and $\sigma_{\min}(\mathcal{O}_\Psi) > 0$ is the minimum singular value of the extended observability matrix $\mathcal{O}_\Psi$ under the side information constraint $\Psi x = 0$. Specifically,

$$\mathcal{O}_\Psi = \begin{bmatrix} \Phi_{\mathcal{I}_h} \\ \Psi \end{bmatrix} = \begin{bmatrix} C_{\mathcal{I}_h} \\ C_{\mathcal{I}_h} A \\ \vdots \\ C_{\mathcal{I}_h} A^{\tau-1} \\ \Psi \end{bmatrix} \in \mathbb{R}^{(|\mathcal{I}_h|\tau+m)\times n}, \tag{20}$$

Proof. Let $z = \hat{x}^* - x(0)$. From the optimality conditions of the perturbed objective function $f(x) = \sum_{i=1}^p \|\Phi_i(x) - Y_i\|_{1/1}$, and using the fact that $\hat{x}^*$ is a minimizer, we can derive:

$$\sum_{i=1}^p \|\Phi_i(\hat{x}^*) - Y_i\|_{1/1} \leq \sum_{i=1}^p \|\Phi_i(x(0)) - Y_i\|_{1/1}.$$

Since $Y_i = \Phi_i(x(0)) + Y_{ai} + V_i$, $\Phi_i(\hat{x}^*) - Y_i = \Phi_i(\hat{x}^*) - \Phi_i(x(0)) - Y_{ai} - V_i = \Phi_i(z) - Y_{a_i} - V_i$.
Thus,

$$\sum_{i=1}^p \|\Phi_i(z) - Y_{a_i} - V_i\|_{1/1} \leq \sum_{i=1}^p \|Y_{a_i} + V_i\|_{1/1}.$$

Separating sensors into two groups: attacked $\mathcal{I}_a$ and non attacked $\mathcal{I}_h$, it comes that

$$\sum_{i\in\mathcal{I}_h} \|\Phi_i(z) - Y_{a_i} - V_i\|_{1/1} + \sum_{i\in\mathcal{I}_a} \|\Phi_i(z) - Y_{a_i} - V_i\|_{1/1} \leq \sum_{i\in\mathcal{I}_h} \|0 + V_i\|_{1/1} + \sum_{i\in\mathcal{I}_a} \|Y_{a_i} + V_i\|_{1/1}.$$

Applying the reverse triangle inequality, it follows that

$$\sum_{i\in\mathcal{I}_h} \|\Phi_i(z)\|_{1/1} - \sum_{i\in\mathcal{I}_a} \|\Phi_i(z)\|_{1/1} \leq 2\sum_{i=1}^p \|V_i\|_{1/1} \leq 2\bar{v}\tau p n.$$

From remark 11, it can be obtained that there exist $p \in (0,1)$, such that

$$p \sum_{i \in \mathcal{I}_h} \|\Phi_i(z)\|_{1/1} > \sum_{i \in \mathcal{I}_a} \|\Phi_i(z)\|_{1/1}.$$

Thus,

$$\sum_{i \in \mathcal{I}_h} \|\Phi_i(z)\|_{1/1} \leq \frac{2}{(1-p)} \bar{v} \tau p n.$$

The $(\Psi, 2l)$-observability condition guarantees that $\mathcal{O}_\Psi$ has full column rank, leading to:

$$\|\mathcal{O}_\Psi z\|_2 \geq \sigma_{\min}(\mathcal{O}_\Psi) \|z\|_2.$$

From the structure of $\mathcal{O}_\Psi$ and $\Psi z = \Psi \hat{x}^* - \Psi x(0) = 0$, it follows that

$$\|\Phi_{\mathcal{I}_h} z\|_2 \geq \sigma_{\min}(\mathcal{O}_\Psi) \|z\|_2$$

Finally, according to the norm equivalence, there exists a constant $c > 0$ such that $\|\cdot\|_{1/1} \geq c\|\cdot\|_2$. Thus, it yields the desired bound (19).

6 Simulation Verification

In the previous section, by introducing two constrained consensus lemmas, we successfully proved the effectiveness of the aforementioned distributed algorithm. In this section, we use Matlab simulations to further verify the effectiveness of the algorithm proposed in the previous section.

6.1 Effectiveness Verification

First, we use a simple example to illustrate the effectiveness of the distributed secure estimation protocol (10). Consider the cyber-physical system (1) with the following parameter matrices:

$$A = \begin{bmatrix} 0.8 & 0.1 & 0.05 \\ 0.1 & 0.7 & 0.15 \\ 0.05 & 0.1 & 0.9 \end{bmatrix},$$

$$C_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, C_2 = \begin{bmatrix} 0 & 0 & 1 \end{bmatrix}, C_3 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}, C_4 = \begin{bmatrix} 0.6 & 0.4 & 0 \\ 0 & 0.6 & 0.4 \end{bmatrix}.$$

For the communication weights, set $a_{ij} = 1$ if i and j is connected, otherwise $a_{ij} = 0$. Then, w_{ij} can calculate from a_{ij}. Set the side information matrix:

$$\Psi = \begin{bmatrix} 1 & 1 & 1 \\ 1 & -1 & 4 \end{bmatrix}.$$

Subject to the side information condition (2), the initial state is selected as $x(0) = [10, -6, -4]^\top$.

The attack vector is set such that half of the sensor values are randomly attacked. Without using prior information, the system cannot successfully estimate the initial state under this condition. For convenience, the eight channels of four sensor clusters are sequentially recorded as Ch1-CH8. Suppose the attacker chooses channel Ch2, Ch3, Ch6, CH7 to randomly inject attack vectors and the attack $a(k)$ is drawn from a normal distribution with mean zero and standard deviation $\sigma = 2$.

Next, we demonstrate the performance of the distributed SSE algorithm with side prior information $\Psi x(0) = \mathbf{0}$. Figure 1 shows the topology of the sensor clusters. Figure 2 shows the logarithmic convergence trend of the estimation error for each sensor cluster in the distributed SSE algorithm. It can be observed that the estimation error for each sensor cluster decreases rapidly.

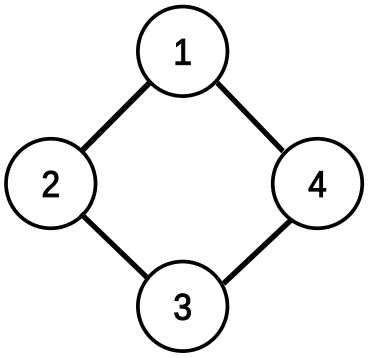

Figure 1. Sensor Cluster Topology

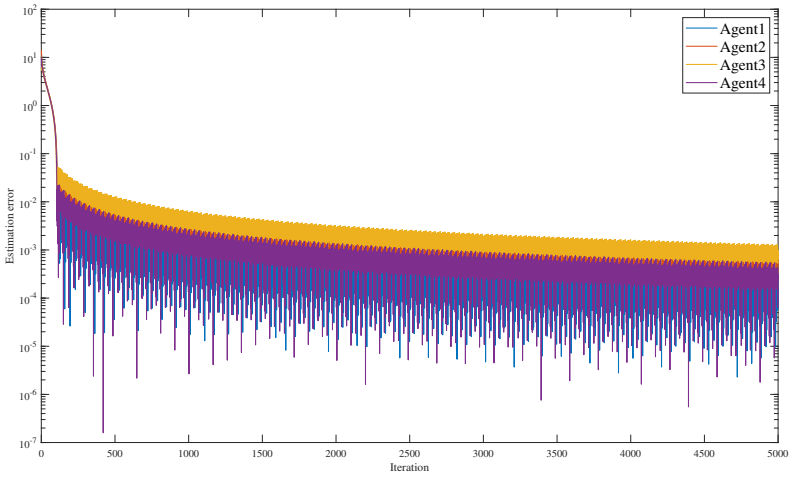

Figure 2. Estimation Error Trend under Side Prior Information

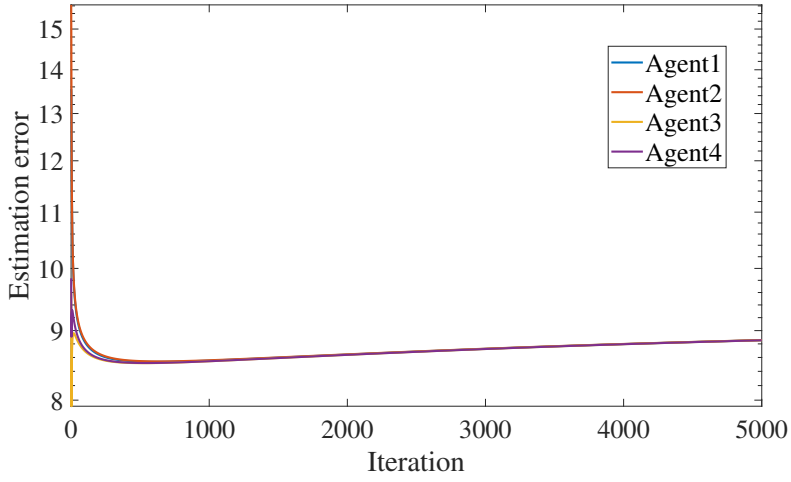

Figure 3. Estimation Error Trend without Side Prior Information

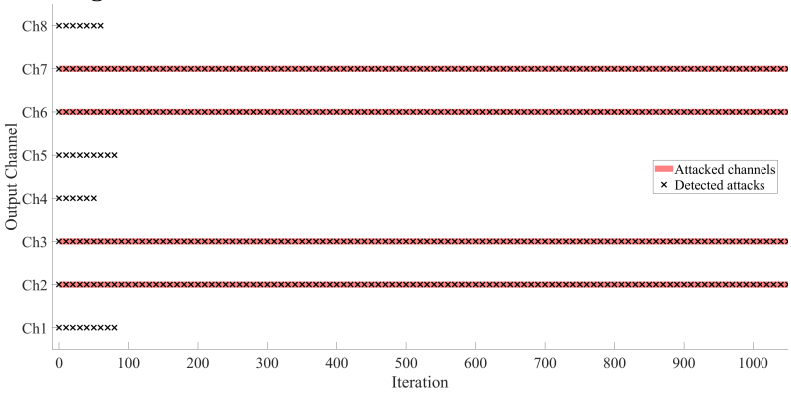

Figure 4. Attack Identification

Figure 3 depicts the evolution of estimation errors for the four sensor clusters under the distributed SSE algorithm without side prior information. It can be observed that the estimation error for each sensor cluster failed to converge to zero, which means the side prior information surely improve system resilience.

Figure 4 shows the detection and localization of the channels under attack in the iteration of the distributed SSE algorithm, where the red horizontal lines mark the true attacked channels and the black

crosses indicate the channels identified as under attack by the algorithm. Since there is no change in all the next iterations, this figure only shows the judgment of the first 1000 iterations. It can be seen that although all channels are considered to be attacked at the beginning, the algorithm successfully located the attacked channel as the number of iterations increased.

Then the following part validates the theoretical robustness analysis provided in Section 5 by examining the performance of the proposed algorithm under bounded measurement noise.

The system parameters remain identical to those in Subsection 6.1 besides the measurement noise $v_i(k)$. Each element of the noise vector $v_i(k)$ is drawn from a uniform distribution over $[-\bar{v}, \bar{v}]$, with the noise bound set to $\bar{v} = 0.5$.

From Figure 5, the simulation demonstrates that in the presence of noise, the estimation error converges to a bounded neighborhood of zero rather than decaying to zero asymptotically.

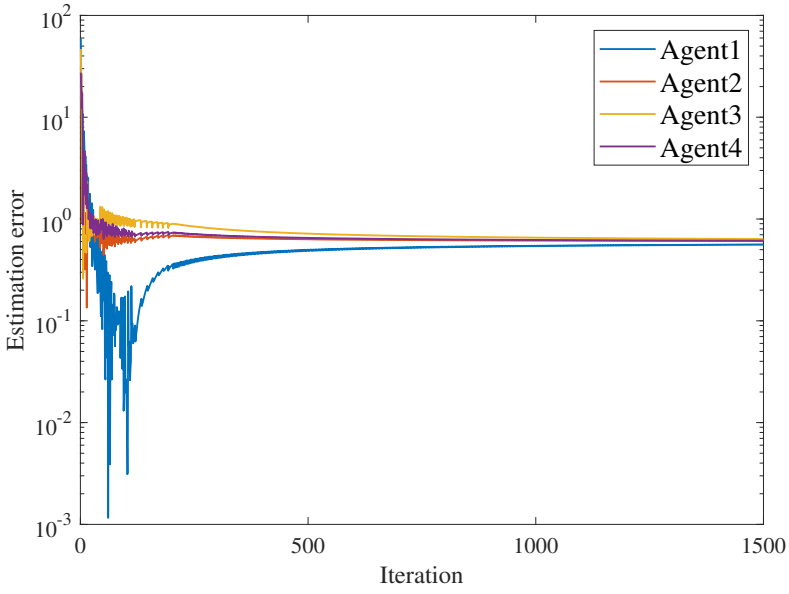

Figure 5. Estimation Error Trend with Measurement Noise

6.2 Estimation Average Success Rate

This subsection aims to validate the robustness of the proposed side-information-based distributed SSE algorithm against varying numbers of attackers. Hence, the following simulations are carried out to evaluate the success rate of SSE under different attacker counts. The simulation considers an initial state dimension $n = 25$ and 10 sensor clusters. In each sensor cluster, there are 3 channels. In numerical simulation, a trial is considered successful if the average reconstructed error $\bar{e} = \frac{1}{10}\sum_{i=1}^{10} \|\hat{x}_i - x(0)| \leq \epsilon$ with $\epsilon = 0.01$. The success rate indicates the proportion of successful trials out of a total of 100 trials.

Figure 6 shows the average success rate over 100 random trials under four different amounts of side prior information, where SI stands for side information and the preceding numbers represent the row rank of the side information matrix Ψ. The solid lines represent the performance of the proposed distributed algorithm enhanced by side information, while the dashed lines correspond to a baseline centralized algorithm utilizing the same side information.

It can be observed that when no side prior information is used (0 SI), the distributed SSE algorithm fails to estimate initial state correctly when the number of attacked output channels exceeds half. When any amount of side prior information is introduced, the algorithm can successfully estimate the initial state even when more than half of the output channels are attacked. Critically, the performance curves for the distributed and centralized approaches are nearly coincident. This indicates that the resilience enhancement gained from side information is essentially preserved in the distributed framework. The

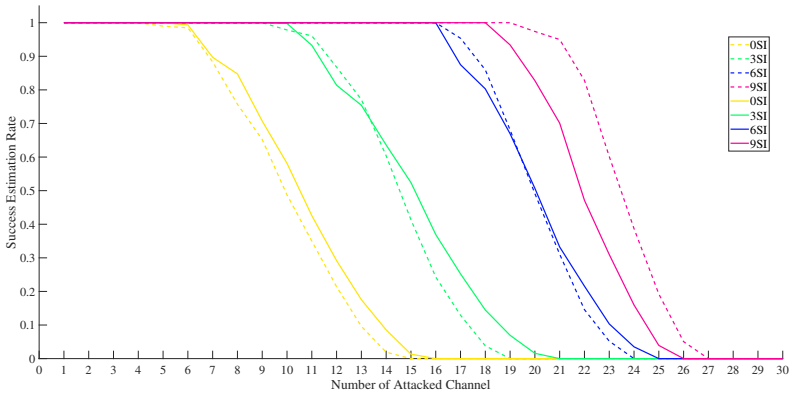

Figure 6. Success Rate of Algorithm in Large-Scale Setting

degradation in attack tolerance due to decentralization is negligible. Furthermore, as the amount of side prior information increases, the algorithm can tolerate a higher number of attacks. This validates the robustness of the algorithm by introducing side information.

7 Conclusion

This paper has presented a solution for enhancing the resilience of distributed SSE for cyber-physical systems by investigating the application of side prior information in distributed algorithms. Through theoretical analysis and numerical simulations, the following conclusions are drawn.

The proposed distributed SSE algorithm based on side prior information can accurately estimate the system's initial state even when more than half of the sensors are compromised, significantly enhancing the system's secure resilience. Theoretical proofs demonstrate that under the $(\Psi, 2l)$-observability condition and the corresponding optimization problem equivalence condition, the algorithm guarantees convergence to the true state. Simulation results validate the algorithm's effectiveness. In small scale system, the algorithm converges rapidly and accurately identifies attack locations. In large scale system, as the amount of side prior information increases, the algorithm tolerates a higher proportion of attacks, exhibiting good resilience.

However, this study has certain limitations. The algorithm performance relies on accurate side prior information, and how to obtain reliable prior information in practical applications requires further exploration. The algorithm cannot deal with time-varying attacks, since the time-varying attacks will destroy the sparsity in Y_a, which lead to failure of optimization problem. Future research directions include: exploring more efficient distributed optimization algorithms to reduce computational complexity, extending the proposed framework to broader application scenarios such as nonlinear systems or time-varying attack.

Acknowledgments

No acknowledgments.

Funding

Funded by Basic Research Program of Jiangsu(Grants No BK20251287)

Conflicts of interest

The author declare no conflicts of interest.

Data availability statement

No data are associated with this article.

Author contribution statement

Zheyi Zhao conducted the theoretical derivation, performed the experiments, and wrote the manuscript. Xuqiang Lei assisted in the inspection of theoretical derivations, and provided revision and proofreading of the paper. Huian Yan participated in the simulation. All authors read and approved the final manuscript.

References

[1] Wen GH and Wang PJ and Lv YZ and et al. Secure consensus of multi-agent systems under denial-of-service attacks. Asian Journal of Control 2023; **25**: 695-709.

[2] Fu XQ and Wen GH and Niu MF and et al. Distributed Secure Filtering Against Eavesdropping Attacks in SINR-Based Sensor Networks. IEEE Trans. Inf. Forensics Security 2024; **19**: 3483–3494.

[3] Ye D and Zhang TY. Summation detector for false data-injection attack in cyber-physical systems. IEEE Trans. Cybern. 2020; **50**: 2338–2345.

[4] Langner R. Stuxnet: Dissecting a Cyberwarfare Weapon. IEEE Security Privacy 2011; **9**: 49–51.

[5] Slay J and Miller M. Lessons learned from the maroochy water breach. International conference on critical infrastructure protection, 2007.

[6] Pultarova T. News Briefing: Cyber security - Ukraine grid hack is wake-up call for network operators. Engineering and Technology 2016; **11**: 12–13.

[7] Wen GH and Yu WW and Yu XH and et al. Complex cyber-physical networks: From cybersecurity to security control. Journal of Systems Science and Complexity 2017; **30**: 46–67.

[8] Zhao D and Wen GH and Wu ZG and et al. Resilient Consensus of Multiagent Systems Under Collusive Attacks on Communication Links. IEEE Transactions on Cybernetics 2024; **54**: 2076–2085.

[9] Zhao D and Ho Daniel and Wen GH. Generalized Graph-Dependent Isolation of Collusive Attacks for Interconnected Systems. IEEE Transactions on Automatic Control 2025; **70**: 2274–2288.

[10] Candes E J and Tao T. Decoding by linear programming. IEEE Trans. Inf. Theory 2005; **51**: 4203–4215.

[11] Shoukry Y and Nuzzo P and Puggelli A and et al. Secure State Estimation For Cyber Physical Systems Under Sensor Attacks: A Satisfiability Modulo Theory Approach. IEEE Trans. Autom. Control 2017; **62**: 4917–4932.

[12] Lu, AY and Yang, GH. A Polynomial-Time Algorithm for the Secure State Estimation Problem Under Sparse Sensor Attacks via State Decomposition Technique. IEEE Trans. Autom. Control 2023; **68**: 7451–7465.

[13] Zhao ZG and Li YZ and Yang Y and et al. Sparse Undetectable Sensor Attacks Against Cyber-Physical Systems: A Subspace Approach. IEEE Trans. Circuits Syst. II, Exp. Briefs 2020; **67**: 2517–2521.

[14] Liu CS and Wu J and Long CN and et al. Dynamic State Recovery for Cyber-Physical Systems Under Switching Location Attacks. IEEE Trans. Control Netw. Syst. 2017; **4**: 14–22.

[15] Chang Y H and Hu Q and Tomlin, C J. Secure estimation based Kalman Filter for cyber-physical systems against sensor attacks. Automatica 2018; **95**: 399–412.

[16] Fawzi H and Tabuada P and Diggavi S. Secure Estimation and Control for Cyber-Physical Systems Under Adversarial Attacks. IEEE Trans. Autom. Control 2014; **59**: 1454–1467.

[17] An LW and Yang GH. State Estimation Under Sparse Sensor Attacks: A Constrained Set Partitioning Approach. IEEE Trans. Autom. Control 2019; **64**: 3861–3868.

[18] An LW and Yang GH. Distributed secure state estimation for cyber physical systems under sensor attacks. Automatica 2019; **107**: 526–538.

[19] Shoukry Y and Tabuada P. Event-Triggered State Observers for Sparse Sensor Noise/Attacks. IEEE Trans. Autom. Control 2016; **61**: 2079–2091.

[20] Lu AY and Yang GH. Distributed Secure State Estimation in the Presence of Malicious Agents. IEEE Trans. Autom. Control 2021; **66**: 2875–2882.

[21] Shinohara T and Namerikawa T and Qu ZH. Resilient Reinforcement in Secure State Estimation Against Sensor Attacks With A Priori Information. IEEE Trans. Autom. Control 2019; **64**: 5024–5038.

[22] Lu, AY and Yang GH. Detection and Identification of Sparse Sensor Attacks in Cyber-Physical Systems With Side Information. IEEE Trans. Autom. Control 2023; **68**: 5349–5364.

[23] Shinohara T and Namerikawa T. Distributed secure state estimation with a priori sparsity information. IET Control Theory Appl. 2022; **16**: 1086–1097.

[24] Nedic A., Ozdaglar A., and Parrilo P. Constrained Consensus and Optimization in Multi-Agent Networks. IEEE Trans. Autom. Control 2010; **55**: 922-938.

Zheyi Zhao received the B.Sc. degree in mathematics from The Chinese University of Hong Kong, Shenzhen, Shenzhen, China, in 2021. Currently, he is actively engaged in his M.Sc. degree, specializing in mathematics at Liaoning Technical University, Fuxin, China. His current research focuses on Secure state estimation and secure control.

Xuqiang Lei received the B.S. degree in the School of Science, Jiangsu University, Zhenjiang, China, in Jun. 2017, and the Ph.D. degree in applied mathematics from Southeast University, Nanjing, China, in Dec. 2024. He is currently an assistant researcher at the School of Mathematics, Southeast University, Nanjing, China. His research interests include cyber-physical systems, distributed secure state monitoring, and resilient consensus control.

Huian Yan received the B.Sc. degree in School of mathematics, Southeast University, Nanjing, China, in Jun.2020. Currently, she is actively engaged in her M.Sc. degree, specializing in School of electrical and control engineering at Liaoning Technical University, Huludao, China. Her current research focuses on Fault-tolerant control of multi-agent systems.