fractal and fractional

MDPI

Article

Resilient Prescribed-Time Safe Optimization for Fractional-Order Multi-Agent Systems Under False Data Injection Attacks

Chao Lu [1,2], Chen Zhang [2], Yajun Xu [1], Pingyuan Yan [1], Zhihan Shi [1,*] and Guangming Zhang [1,2]

[1] School of Electrical and Energy Engineering, Nantong Institute of Technology, Yongxing Road, Nantong 226001, China; lc-1206@njtech.edu.cn (C.L.); yajunxu@ntit.edu.cn (Y.X.); pyyan@ntit.edu.cn (P.Y.); zgm@njtech.edu.cn (G.Z.)

[2] School of Mechanical and Power Engineering, Nanjing Tech University, Puzhu Road, Nanjing 211816, China; 202362071170@njtech.edu.cn

* Correspondence: 20256115@ntit.edu.cn

Abstract

This paper studies resilient safe distributed optimization with practical prescribed-time performance for fractional-order multi-agent systems under false data injection attacks. Caputo dynamics are used to represent memory-dependent agent behavior. A local trimming mechanism is combined with gradient feedback, auxiliary coordination, a bounded time-varying gain, and a barrier-type safety correction. In contrast to an ideal singular prescribed-time design, the proposed bounded gain drives the normal-agent errors into an explicitly characterized neighborhood of the global optimizer at the assigned time, provided that a verifiable gain matrix is positive definite. Explicit residual bounds are derived in terms of the attack amplitudes, the trimming level, and the retained-neighbor redundancy. A fractional extremum argument is further used to establish forward invariance of the safe interval. The analysis proves boundedness of the physically relevant closed-loop signals, safety preservation, practical prescribed-time convergence, and robustness against bounded disturbances. Simulations on a sparse six-agent network demonstrate the roles of resilient information processing and barrier correction without requiring all-to-all communication.

Keywords: fractional-order multi-agent systems; false data injection attacks; safe distributed optimization; prescribed-time control; resilient control; barrier function

1. Introduction

Distributed optimization enables networked agents to minimize a global objective while each agent uses only its local cost and neighboring information [1,2]. It has become relevant to networked control, smart grids, and autonomous systems [3–5]. In contrast to ordinary consensus, distributed optimization must simultaneously coordinate the agents and preserve the descent direction associated with the aggregate cost.

Fractional-order dynamics provide a natural description of hereditary, nonlocal, and memory-dependent behavior [6]. These properties are useful in complex networked systems but make attack residues and transient errors more persistent than in integer-order models. Existing fractional-order multi-agent studies have considered containment, consensus, and distributed optimization under uncertainty or disturbances [7–10]. However, cyber resilience, safety constraints, and a designer-assigned transient time scale have rarely been treated within one fractional-order optimization framework.

Communication attacks can corrupt both the consensus signal and the optimization direction. False data injection, deception, Byzantine behavior, denial-of-service, replay, and

Check for updates

Academic Editor: Costas Psychalinos

Received: 2 July 2026
Revised: 27 July 2026
Accepted: 28 July 2026
Published: 29 July 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

mobile malicious attacks have therefore motivated resilient coordination and optimization methods [11–15]. At the same time, safe transient behavior is essential when decision variables represent physical quantities. Barrier Lyapunov functions and control barrier functions provide useful tools for enforcing state constraints [16,17], whereas prescribed-time mechanisms can accelerate cooperative decisions around a designer-assigned time [18–21]. Combining these ingredients is nontrivial because filtering changes the effective graph, the bounded time-varying gain yields only practical convergence, and the fractional memory must be considered in the safety argument.

This paper develops a resilient safe optimization protocol for scalar Caputo fractional-order agents subject to bounded additive attacks on transmitted state and auxiliary information. The main contributions are as follows:

1. A unified fractional-order framework is established that combines local resilient trimming, distributed optimization, a bounded prescribed-time gain, and a barrier-type safety correction. The result is explicitly stated as practical prescribed-time convergence to an adjustable neighborhood rather than exact zero-error convergence at the assigned time.
2. A retained-data decomposition is derived with explicit residual bounds depending on the local attack bound q, the minimum retained-neighbor number, and the attack amplitudes. A quantitative positive-definiteness condition is then provided for controller and Lyapunov parameters, replacing the previous qualitative gain requirement.
3. Safety preservation is proved by a fractional extremum principle and a first-hitting-time contradiction. The relationship among the assigned time, the residual set, the gain bound, and the resulting error radius is made explicit through a Mittag–Leffler estimate.
4. Comparative ablations demonstrate the necessity of the resilient and safety modules. A separate related-work comparison and a discussion of attack scope, multidimensional extension, and sensitivity to an incorrectly selected q clarify the applicability and limitations of the method.

The remainder of this paper is organized as follows. Section 2 reviews related methods. Section 3 classifies attack models and defines the scope of this study. Section 4 formulates the problem. Section 5 presents the resilient safe optimization protocol and quantitative design conditions. Section 6 gives the convergence and safety analysis. Section 7 reports the simulations, and Section 8 discusses the results and limitations. Section 9 concludes the paper.

2. Related Work

2.1. Fractional-Order Distributed Optimization and Time-Constrained Coordination

Distributed optimization for integer-order agents is well-established [1,2]. Recent studies have extended optimization and coordination to fractional-order multi-agent systems, including finite-time distributed optimization, delayed double-integrator models, and neural adaptive coordination [7–10]. These results demonstrate the importance of fractional memory but do not simultaneously address malicious communication data and state safety.

Prescribed-time coordination has been studied for consensus, containment, and constrained distributed optimization [18–20]. Singularity-free time-varying gains have also been investigated to reduce the numerical burden caused by conventional blow-up functions [21]. The present paper follows this practical singularity-free direction: the bounded gain is used to meet a designer-selected transient accuracy at T_c, rather than to claim exact convergence at T_c.

2.2. Resilient Consensus and Distributed Optimization

Mean-subsequence-reduced and local filtering strategies are classical tools for resilient consensus under locally bounded adversaries [12,22]. Resilient distributed optimization has been developed for adversarial and Byzantine agents in both scalar and multidimensional settings [13,14,23]. These methods provide important graph-theoretic and filtering foundations. Nevertheless, they mainly concern integer-order updates and do not include the combination of fractional memory, prescribed transient performance, and barrier-based state safety studied here.

Mobile malicious attacks are more demanding because the compromised identities can change over time. Representative studies have established resilient scalar or vector consensus over directed and random dynamic networks [15,24]. Their objectives, attack processes, and graph conditions differ from the bounded static-transmitter false-data model considered in this paper. The comparison is discussed further in Section 3.

2.3. Comparison with Representative Methods

Table 1 summarizes representative contributions. The table is intended to position the present problem rather than claim universal superiority. Direct numerical ranking is generally inappropriate because the cited methods use different dynamics, threat models, objectives, and network assumptions.

Table 1. Comparison with representative resilient and time-constrained coordination methods.

Method	Fractional Dynamics	Optimization	Malicious Data	State Safety	Assigned Time	Decision Dimension
Wang et al. [18]	No	No	No	No	Exact prescribed time	Scalar
Gong et al. [9]	Yes	Yes	No	No	Finite time	Scalar
Zhao et al. [13]	No	Yes	Adversarial agents	No	Asymptotic	Scalar
Su and Vaidya [14]	No	Yes	Byzantine agents	No	Asymptotic	Scalar
Kuwarananchareon et al. [23]	No	Yes	Byzantine agents	No	Asymptotic	Vector
Shang [15]	No	No	Mobile malicious agents	No	Asymptotic	Vector
This work	Yes	Yes	Bounded FDI data	Yes	Practical prescribed time	Scalar; box extension

3. Attack Models and Scope

Cyber attacks on multi-agent systems differ in both mechanism and location. Additive false data injection and deception attacks modify transmitted measurements or coordination variables. Byzantine agents may send arbitrary and mutually inconsistent messages. Denial-of-service attacks suppress communication, replay attacks substitute previously recorded data, and mobile malicious attacks allow the compromised identity to change over time [11,15,25–27]. Table 2 clarifies the scope of the present analysis.

The protocol is therefore evaluated under a static locally bounded set of attacked transmitters. The mobile-attack results in [15,24] demonstrate that attacker mobility changes both the filtering rule and the required graph robustness. Extending the present theorem to mobile attacks would additionally require accounting for the history of previously compromised nodes in the Caputo derivative. For this reason, mobile attacks are discussed and compared, but are not claimed to be covered by the present proof or simulations.

Table 2. Attack taxonomy and coverage of the present protocol.

Attack Type	Primary Effect	Covered Here	Comment
Bounded additive FDI/deception	Corrupts transmitted values	Yes	Applied to state and auxiliary channels; amplitudes are bounded but unknown to the controller.
Intermittent or step-like FDI	Time-varying corruption	Yes	Included when representable by bounded additive signals.
Byzantine attack	Arbitrary inconsistent messages	Partly	Extreme values can be attenuated, but arbitrary unbounded or coordinated Byzantine behavior is outside the theorem.
Denial-of-service	Removes communication	No	Requires availability and switching-topology analysis.
Replay attack	Reuses delayed historical data	No	Fractional memory and communication delay must be modeled explicitly.
Mobile malicious attack	Changes compromised identities	No	The current attacked-source set is static; mobile attacks require time-varying threat and robustness conditions.
Direct actuator/plant attack	Modifies physical dynamics	No	This paper considers communication-layer corruption only.

4. Preliminaries and Problem Formulation

4.1. Graph Theory and Notation

Let $\mathbb{R}$ denote the set of real numbers. For a vector z, $\|z\|$ is its Euclidean norm. Consider N agents connected by an undirected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E}, A)$, where $\mathcal{V} = \{1, \ldots, N\}$, $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$, and $A = [a_{ij}] \in \mathbb{R}^{N \times N}$. The neighbor set of agent i is

$$\mathcal{N}_i = \{j \in \mathcal{V} : a_{ij} > 0\}. \tag{1}$$

The Laplacian is denoted by L. Let

$$\Pi = I_N - \frac{1}{N}\mathbf{1}\mathbf{1}^\top \tag{2}$$

be the orthogonal projector onto the disagreement space. The sets of normal and attacked transmitters are denoted by $\mathcal{V}_n$ and $\mathcal{V}_a$, respectively.

4.2. Fractional-Order Agent Dynamics

For $\alpha \in (0, 1)$, the Caputo derivative is

$${}^{C}D_t^{\alpha} x(t) = \frac{1}{\Gamma(1-\alpha)} \int_0^t \frac{\dot{x}(\tau)}{(t-\tau)^{\alpha}}\, d\tau. \tag{3}$$

Each agent obeys

$${}^{C}D_t^{\alpha} x_i(t) = u_i(t) + d_i(t), \qquad i \in \mathcal{V}, \tag{4}$$

where $x_i \in \mathbb{R}$, $u_i \in \mathbb{R}$, and d_i is a bounded disturbance.

The following two fractional inequalities are used.

Lemma 1. *For a differentiable vector z and a constant symmetric positive-semidefinite matrix P,*

$$\frac{1}{2}{}^{C}D_t^{\alpha}\left(z^\top P z\right) \le z^\top P\, {}^{C}D_t^{\alpha} z. \tag{5}$$

Lemma 2 (Fractional extremum principle)**.** *Let y be continuously differentiable on $(0, T]$ and continuous on $[0, T]$. If y attains its maximum at $t^\star \in (0, T]$, then ${}^C D_t^\alpha y(t^\star) \geq 0$. If it attains its minimum at $t^\star$, then ${}^C D_t^\alpha y(t^\star) \leq 0$.*

Proof. Integration by parts gives

$$ {}^C D_t^\alpha y(t^\star) = \frac{y(t^\star) - y(0)}{\Gamma(1-\alpha)(t^\star)^\alpha} + \frac{\alpha}{\Gamma(1-\alpha)} \int_0^{t^\star} \frac{y(t^\star) - y(\tau)}{(t^\star - \tau)^{\alpha+1}}\, d\tau. $$

Both terms are nonnegative at a maximum and nonpositive at a minimum. □

4.3. Distributed Optimization and Safety

Each agent knows a local function $f_i : \mathbb{R} \to \mathbb{R}$. The global problem is

$$ \min_{x \in \Omega} F(x) = \sum_{i=1}^{N} f_i(x), \qquad x^* = \arg\min_{x \in \Omega} F(x). \tag{6} $$

The safe set is

$$ \Omega = (x_{\min}, x_{\max}), \qquad x_{\min} < x_i(t) < x_{\max}. \tag{7} $$

4.4. False Data Injection Model

The information transmitted from j to i is

$$ x_{j\to i}^a(t) = x_j(t) + \delta_{ij}^x(t), \tag{8} $$

$$ \lambda_{j\to i}^a(t) = \lambda_j(t) + \delta_{ij}^\lambda(t), \tag{9} $$

where λ_j is an auxiliary coordination variable. The controller does not know the attack values or the identities of attacked transmitters.

Assumption 1. *For each normal agent, at most q neighbors are attacked and $|\mathcal{N}_i| > 2q$. Consequently, the retained sets introduced below are nonempty. The integer q is a design-side threat bound, not an online attack estimate.*

Assumption 2. *Let $L_R^x(t)$ and $L_R^\lambda(t)$ denote the normalized Laplacian-like operators induced by the retained state and auxiliary data. Their symmetric parts satisfy, for all $y \in \mathbf{1}^\perp$,*

$$ y^\top \operatorname{sym}(L_R^s(t)) y \geq \underline{\ell}_s \|y\|^2, \qquad \|L_R^s(t)\| \leq \overline{\ell}_s, \qquad s \in \{x, \lambda\}, \tag{10} $$

where $\underline{\ell}_s > 0$ and $\overline{\ell}_s < \infty$. This is a uniform robust-connectivity condition on the graph after trimming.

Assumption 3. *Each f_i is continuously differentiable and m_i-strongly convex, and ∇f_i is L_i-Lipschitz continuous. Define*

$$ m_f = \min_i m_i > 0, \qquad L_f = \max_i L_i. $$

Then, F has a unique optimizer x^* and $\sum_i \nabla f_i(x^*) = 0$.

Assumption 4. *There are constants $\bar{\delta}_x, \bar{\delta}_\lambda, \bar{d} > 0$ such that*

$$ |\delta_{ij}^x(t)| \leq \bar{\delta}_x, \quad |\delta_{ij}^\lambda(t)| \leq \bar{\delta}_\lambda, \quad |d_i(t)| \leq \bar{d}. $$

Moreover, $x_i(0), x^* \in (x_{\min}, x_{\max})$, and the initial projected auxiliary variable $\Pi\lambda(0)$ belongs to a known compact set.

Remark 1. *Assumption 1 only guarantees local redundancy and nonempty retained sets; it does not imply that every removed value is malicious. The positive coercivity used in the proof is supplied by Assumption 2. Thus, the roles of local attack sparsity and post-trimming graph robustness are distinct.*

5. Resilient Prescribed-Time Safe Optimization Protocol

5.1. Local Trimming and Explicit Residual Bounds

Agent i compares each received state value with x_i, discards up to q largest values above x_i, and discards up to q smallest values below x_i. If fewer than q values occur on one side, all values on that side are discarded. The retained sets are $\mathcal{R}_i^x(t)$ and $\mathcal{R}_i^\lambda(t)$. Define

$$\xi_i^x = \frac{1}{|\mathcal{R}_i^x|} \sum_{j \in \mathcal{R}_i^x} \left(x_i - x_{j\to i}^a \right), \tag{11}$$

$$\xi_i^\lambda = \frac{1}{|\mathcal{R}_i^\lambda|} \sum_{j \in \mathcal{R}_i^\lambda} \left(\lambda_i - \lambda_{j\to i}^a \right). \tag{12}$$

Let $r_{\min} = \inf_{i,t,s} |\mathcal{R}_i^s(t)| \geq 1$. In stacked form,

$$\xi^x = L_R^x(t)x + r_x(t), \qquad \xi^\lambda = L_R^\lambda(t)\lambda + r_\lambda(t), \tag{13}$$

where the residuals contain only retained attack contributions.

Lemma 3. *Under Assumptions 1 and 4,*

$$\|r_x(t)\| \leq \bar{r}_x := \sqrt{N}\frac{q}{r_{\min}}\bar{\delta}_x, \qquad \|r_\lambda(t)\| \leq \bar{r}_\lambda := \sqrt{N}\frac{q}{r_{\min}}\bar{\delta}_\lambda. \tag{14}$$

Under Assumption 2, for $e = \Pi x$,

$$e^\top \xi^x \geq \frac{\underline{\ell}_x}{2}\|e\|^2 - \frac{\bar{r}_x^2}{2\underline{\ell}_x}. \tag{15}$$

Proof. For each normal agent, no more than q retained entries can be attacked. Hence

$$|r_i^x| \leq \frac{q}{|\mathcal{R}_i^x|}\bar{\delta}_x \leq \frac{q}{r_{\min}}\bar{\delta}_x,$$

and the first bound follows after stacking. The auxiliary bound is identical. Since $L_R^x \mathbf{1} = 0$,

$$e^\top \xi^x = e^\top L_R^x e + e^\top r_x \geq \underline{\ell}_x\|e\|^2 - \bar{r}_x\|e\|.$$

Young's inequality gives (15). □

Remark 2. *The lemma does not claim that trimming identifies attacks. It quantifies the worst retained corruption. Increasing q may reduce the number of potentially malicious values, but it also decreases $r_{\min}$ and can weaken the post-trimming connectivity margin $\underline{\ell}_s$.*

5.2. Bounded Prescribed-Time Gain

The gain is

$$\mu(t) = \begin{cases} \min\left\{ \mu_{\max}, \mu_0 + \mu_1 \left(\dfrac{t}{\max\{T_c - t, \varepsilon_T\}} \right)^{\kappa} \right\}, & 0 \le t < T_c, \\ \mu_{\max}, & t \ge T_c, \end{cases} \tag{16}$$

where all parameters are positive. Since $\mu(t)$ is bounded, T_c prescribes a practical transient accuracy rather than exact zero-error convergence.

5.3. Barrier-Type Safety Correction

Define

$$B_i(x_i) = -\ln(x_i - x_{\min}) - \ln(x_{\max} - x_i) \tag{17}$$

and

$$u_i^s = k_s \left[\frac{1}{(x_i - x_{\min})^2} - \frac{1}{(x_{\max} - x_i)^2} \right], \qquad k_s > 0. \tag{18}$$

The term is positive near the lower boundary and negative near the upper boundary.

5.4. Distributed Controller

The controller is

$$u_i = -\mu(t) \left[k_g \nabla f_i(x_i) + k_x \xi_i^x + k_\lambda \xi_i^\lambda \right] - k_r \tanh(4\xi_i^x) + u_i^s, \tag{19}$$

with

$${}^{C}D_t^{\alpha} \lambda_i = \mu(t) k_d \xi_i^x. \tag{20}$$

Only $\Pi\lambda$ affects the disagreement term; a common offset of all auxiliary variables has no effect on the controller.

For implementation, the complete distributed optimization procedure is summarized in Algorithm 1, where the resilient information processing, bounded prescribed-time gain, safety correction, and controller update are executed sequentially by each normal agent.

The overall framework is shown in Figure 1.

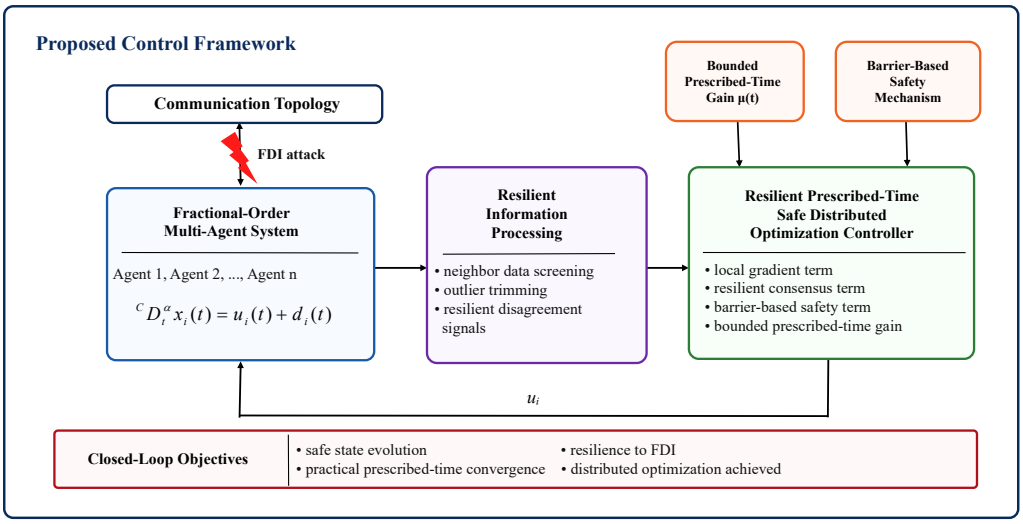


Figure 1. Overall control framework of the resilient safe distributed optimization method.

Algorithm 1 Resilient prescribed-time safe distributed optimization algorithm

1: Initialize $x_i(0) \in (x_{\min}, x_{\max})$ and $\lambda_i(0)$.
2: Select T_c, q, the gain profile, and controller gains.
3: **for** each normal agent i **do**
4: Receive $x^a_{j\to i}$ and $\lambda^a_{j\to i}$.
5: Apply the local trimming rule.
6: Compute ξ^x_i, ξ^λ_i, $\mu(t)$, and u^s_i.
7: Apply (19) and update (20).
8: **end for**

5.5. Quantitative Gain Conditions

Let $\sigma > 0$, $0 < \chi < \sqrt{\sigma}$, and $\varepsilon_q > 0$. Set

$$\bar{\ell} = \max\{\bar{\ell}_x, \bar{\ell}_\lambda\},$$

and define

$$\begin{aligned} q_o &= k_g m_f - \chi k_g L_f - \varepsilon_q, \\ q_e &= k_x \underline{\ell}_x - \chi k_d \bar{\ell}_x - \varepsilon_q, \\ q_\lambda &= \chi k_\lambda \underline{\ell}_\lambda - \varepsilon_q, \\ q_c &= \frac{1}{2}\Big[(k_\lambda + \sigma k_d)\bar{\ell} + \chi k_x \bar{\ell}_x\Big]. \end{aligned} \tag{21}$$

A conservative sufficient condition is

$$q_o > 0, \qquad q_e > 0, \qquad q_\lambda > 0, \qquad q_e q_\lambda > q_c^2. \tag{22}$$

Equivalently,

$$Q = \begin{bmatrix} q_o & 0 & 0 \\ 0 & q_e & -q_c \\ 0 & -q_c & q_\lambda \end{bmatrix} \succ 0. \tag{23}$$

The gains $k_s > 0$ and $k_r > 0$ are finite. The safety gain does not enter Q because it is treated through the invariance argument. The bounded hyperbolic-tangent term contributes a finite amount to the residual constant. Conditions (22) can be checked directly once the strong-convexity, Lipschitz, and retained-graph bounds are available.

Remark 3 (Practical tuning). *One may first select σ and a small χ, then increase k_g until $q_o > 0$, choose k_x and k_d so that $q_e > 0$, and finally increase k_λ until the determinant condition is satisfied. Larger k_r improves local attenuation of residual corruption but may increase control effort. Larger k_s strengthens the inward safety action near the boundary.*

5.6. Extension to Multidimensional Decisions

For $x_i \in \mathbb{R}^p$ and a box

$$\Omega_p = \prod_{\ell=1}^{p} (x_{\min,\ell}, x_{\max,\ell}),$$

the barrier and safety correction can be applied componentwise:

$$B_i(x_i) = -\sum_{\ell=1}^{p} [\ln(x_{i\ell} - x_{\min,\ell}) + \ln(x_{\max,\ell} - x_{i\ell})],$$

$$[u^s_i]_\ell = k_s \left[\frac{1}{(x_{i\ell} - x_{\min,\ell})^2} - \frac{1}{(x_{\max,\ell} - x_{i\ell})^2} \right].$$

The graph terms extend with $L_R^s \otimes I_p$, and the proof uses the same quadratic and extremum arguments componentwise. This extension covers box constraints; arbitrary coupled safe sets would require a vector barrier or a quadratic-program safety filter and are outside the present scope.

6. Stability and Safety Analysis

Theorem 1. *Suppose Assumptions 1–4 hold and the gains satisfy (22). Then, the safe interval (7) is forward invariant. The state error $\tilde{x} = x - x^*\mathbf{1}$, the consensus error Πx, the projected auxiliary variable $\Pi\lambda$, and the control inputs remain bounded. Moreover, there are computable constants $c_Q > 0$ and $\Delta \geq 0$ such that*

$$ {}^{C}D_t^{\alpha} V_0(t) \leq -c_Q \mu(t) V_0(t) + \Delta. \tag{24}$$

Consequently,

$$ V_0(T_c) \leq V_0(0) E_{\alpha}(-c_Q \mu_0 T_c^{\alpha}) + \frac{\Delta}{c_Q \mu_0} \left[1 - E_{\alpha}(-c_Q \mu_0 T_c^{\alpha})\right]. \tag{25}$$

Thus, if the right-hand side of (25) is no larger than a prescribed tolerance ε_V, the normal agents enter the corresponding neighborhood of x^* by T_c. This is practical prescribed-time convergence. Under bounded disturbances, the errors are ultimately bounded.

Proof. Let

$$ \tilde{x} = x - x^*\mathbf{1}, \qquad e = \Pi x, \qquad \nu = \Pi\lambda, $$

and define $z = \mathrm{col}(\tilde{x}, \nu)$. Consider

$$ V_0 = \frac{1}{2} z^{\top} P z, \qquad P = \begin{bmatrix} I_N & \chi\Pi \\ \chi\Pi & \sigma I_N \end{bmatrix}. \tag{26}$$

Because $\sigma > \chi^2$, $P \succ 0$. Hence,

$$ \frac{\lambda_{\min}(P)}{2} \|z\|^2 \leq V_0 \leq \frac{\lambda_{\max}(P)}{2} \|z\|^2. $$

Using Lemma 1, the dynamics, and the decomposition (13), the nominal terms can be grouped into the average optimization error, the disagreement error e, and the projected auxiliary error ν. Strong convexity gives

$$ \tilde{x}^{\top}(g(x) - g(x^*\mathbf{1})) \geq m_f \|\tilde{x}\|^2, $$

where $g(x) = \mathrm{col}(\nabla f_1(x_1), \ldots, \nabla f_N(x_N))$. The constant vector $g(x^*\mathbf{1})$ has zero sum and contributes only a bounded cross term. Assumption 2, Lemma 3, and Young's inequality then yield

$$ {}^{C}D_t^{\alpha} V_0 \leq -\mu(t) \begin{bmatrix} \|\tilde{x}\| \\ \|e\| \\ \|\nu\| \end{bmatrix}^{\top} Q \begin{bmatrix} \|\tilde{x}\| \\ \|e\| \\ \|\nu\| \end{bmatrix} + \Delta, \tag{27}$$

where Q is given in (23). The finite constant Δ contains the explicit retained-attack bounds (14), the disturbance bound $\bar{d}$, the bounded term $k_r \tanh(4\xi_i^x)$, and the constant local-gradient mismatch at x^*. Unlike the earlier qualitative argument, positive dissipation follows from the checkable condition $Q \succ 0$.

Let $\lambda_Q = \lambda_{\min}(Q)$. From (26) and (27),

$$^{C}D_t^{\alpha} V_0 \leq -\frac{2\lambda_Q}{\lambda_{\max}(P)}\mu(t)V_0 + \Delta.$$

Therefore, Equation (24) holds with

$$c_Q = \frac{2\lambda_Q}{\lambda_{\max}(P)}.$$

Because $\mu(t) \geq \mu_0$ on $[0, T_c]$, the fractional comparison principle gives (25). Furthermore,

$$\|z(T_c)\| \leq \sqrt{\frac{2}{\lambda_{\min}(P)}\left[V_0(0)E_{\alpha}(-c_Q\mu_0 T_c^{\alpha}) + \frac{\Delta}{c_Q\mu_0}\right]}.$$

This expression explicitly connects the assigned time, gain condition, attack/disturbance residual, and achievable error radius.

It remains to establish safety. Define

$$a_i = x_i - x_{\min}, \qquad b_i = x_{\max} - x_i.$$

For every interior point,

$$\frac{\partial B_i}{\partial x_i}u_i^s = -k_s\frac{(a_i - b_i)^2(a_i + b_i)}{a_i^3 b_i^3} \leq 0.$$

Suppose that x_i reaches the lower boundary for the first time at $t^{\star}$. On $[0, t^{\star})$, all nonsafety terms in (19) are bounded by the preceding estimate and Assumptions 3 and 4, whereas $u_i^s \to +\infty$ as $x_i \to x_{\min}^{+}$. Hence, there exists a boundary layer in which $^{C}D_t^{\alpha} x_i > 0$. At the first lower-boundary contact, however, x_i attains a minimum and Lemma 2 requires $^{C}D_t^{\alpha} x_i(t^{\star}) \leq 0$, a contradiction. At a first upper-boundary contact, $u_i^s \to -\infty$, while the extremum principle requires a nonnegative Caputo derivative at the maximum, again a contradiction. Therefore, $x_i(t) \in (x_{\min}, x_{\max})$ for all $t \geq 0$.

The boundedness of z, the safe state, and the disagreement signals implies bounded control inputs. The projected auxiliary variable is the physically relevant part because only differences of λ_i enter the controller. This completes the proof. □

Remark 4. *The phrase "practical prescribed-time" has a precise meaning in Theorem 1: the designer selects T_c and a tolerance ε_V, and then chooses gains so that (22) and the bound (25) hold. The theorem does not claim exact zero-error convergence at T_c or global rejection of arbitrary unbounded attacks.*

7. Numerical Simulations

This section illustrates the proposed method through numerical simulations. The experiments are intended to assess the internal modules under a common fractional-order plant; they do not constitute a universal numerical ranking against methods developed for different dynamics and threat models. The fractional-order system is solved by the Adams–Bashforth–Moulton predictor–corrector scheme. This method is suitable for Caputo fractional-order dynamics because it approximates the memory integral by using historical right-hand-side information. The theoretical design is stated for N agents. In the simulation, $N = 6$ is selected for clear visualization and comparison, and the local cost functions are chosen as $f_i(x_i) = \frac{1}{2}(x_i - p_i)^2$, where $p = [-2, -1, 0, 1, 2, 3]^T$. Therefore, the global optimizer is $x^* = 0.5$. The safety interval is $0 < x_i(t) < 1$.

A sparse connected communication topology is adopted as

$$A = \begin{bmatrix} 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

This topology is connected but not complete. Therefore, the simulation does not rely on all-to-all communication. The attacked transmitter is chosen as agent 6. The FDI attack signals are selected as a combination of sinusoidal and step components, which represents a persistent time-varying attack. The fractional order is set as $\alpha = 0.82$, the simulation step size is $h = 0.02$ s, the simulation horizon is $T = 12$ s, and the prescribed time is $T_c = 5.5$ s. The trimming parameter is $q = 1$. The initial states are $x(0) = [0.08, 0.92, 0.25, 0.75, 0.15, 0.85]^T$ and $\lambda(0) = 0$. The controller gains are chosen as $k_g = 0.80$, $k_x = 2.00$, $k_\lambda = 0.80$, $k_d = 0.80$, $k_r = 0.12$, and $k_s = 0.0030$. For the bounded prescribed-time gain, the parameters are selected as $\mu_0 = 1.0$, $\mu_1 = 0.70$, $\kappa = 1.10$, $\mu_{\max} = 8.0$, and $\varepsilon_T = 0.05$. For numerical implementation, a small barrier regularization parameter $\varepsilon_b = 0.03$ is used in the denominator of the barrier-related terms to avoid numerical overflow extremely close to the safety boundary. This regularization is only used in simulation and does not change the theoretical safety mechanism.

The value $q = 1$ matches the assumed single attacked neighbor in the chosen topology. Section 8 explains the consequences of underestimating or overestimating this value. No modification of the simulation program is required for the theoretical clarification added in the revision.

To further quantify the effectiveness of the proposed design, four same-model cases are compared: the proposed method, the method without resilient information processing, the method without the safety correction term, and the proposed method under small external disturbances. The corresponding quantitative results are listed in Table 3. In this table, "Max. error" denotes the worst final optimization error among all agents, calculated by $\max_i |x_i(T) - x^*|$. "Mean error" is the mean absolute final optimization error, calculated by $\frac{1}{N}\sum_{i=1}^{N} |x_i(T) - x^*|$, which reflects the average optimization accuracy of all agents. "RMS error" is computed as $\sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i(T) - x^*)^2}$ and is used to evaluate the overall final optimization performance. "RMS consensus" is defined as $\sqrt{\frac{1}{N}\sum_{i=1}^{N}(x_i(T) - \bar{x}(T))^2}$, which measures the final agreement level among agents. "Min. margin" is computed as $\min_t \min_i \{x_i(t) - x_{\min}, x_{\max} - x_i(t)\}$. A positive value indicates that all agents remain inside the safe interval during the whole simulation, whereas a negative value indicates constraint violation. "Violations" denotes the number of sampling instants at which the minimum safety margin is negative.

Table 3. Quantitative comparison of different simulation cases.

Case	Max. Error	Mean Error	RMS Error	RMS Consensus	Min. Margin	Violations
Proposed method	0.0142	0.0066	0.0085	0.0084	0.0577	0
No resilience	0.4645	0.4281	0.4350	0.0774	−0.1054	31
No safety	0.0138	0.0064	0.0083	0.0082	−0.0670	111
Proposed + disturbance	0.0147	0.0067	0.0087	0.0086	0.0578	0

The simulation results are presented in Figures 2–10. Figure 2 shows the communication topology under FDI attacks, where the attacked transmitter is marked in red. Figure 3 gives the injected attack signals in the state and auxiliary-variable channels. These two figures describe the considered networked attack scenario and the time-varying corrupted information used in the subsequent comparisons.

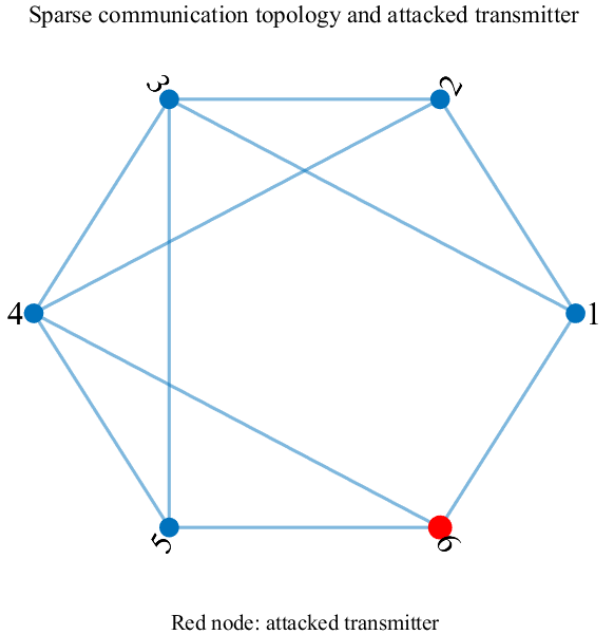


Figure 2. Communication topology under FDI attacks.

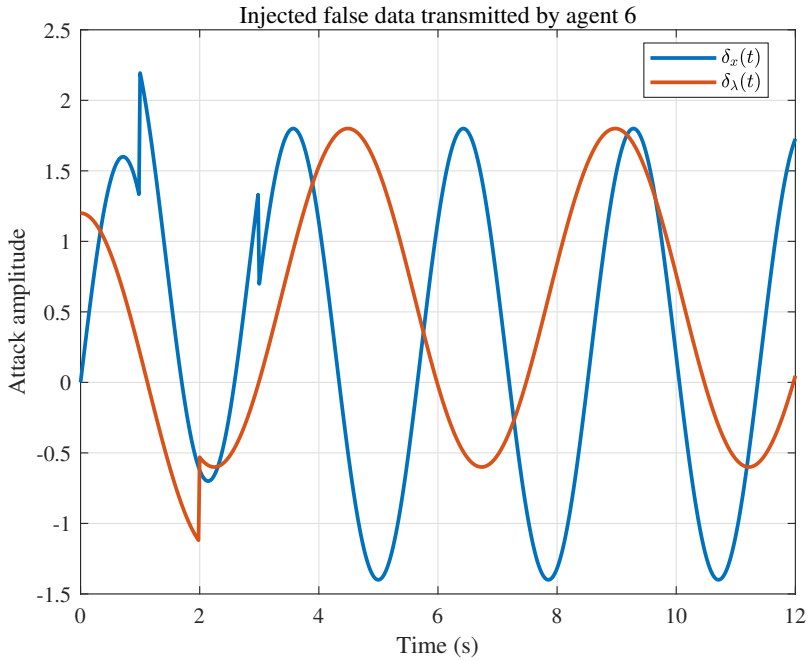


Figure 3. FDI attack signals injected into transmitted data.

Figures 4–7 show the main convergence and safety performance of the proposed method. As shown in Figure 4, all agent states remain inside the prescribed safety interval and approach the global optimizer. Figures 5 and 6 further show that the raw optimization errors and consensus errors converge to small neighborhoods of zero. The positive safety

margin in Figure 7 confirms that the state constraints are preserved during the whole transient process. In contrast, the negative margins of the no-safety and no-resilience cases show that the resilient information processing and the safety correction term are both necessary for maintaining constraints under FDI attacks.

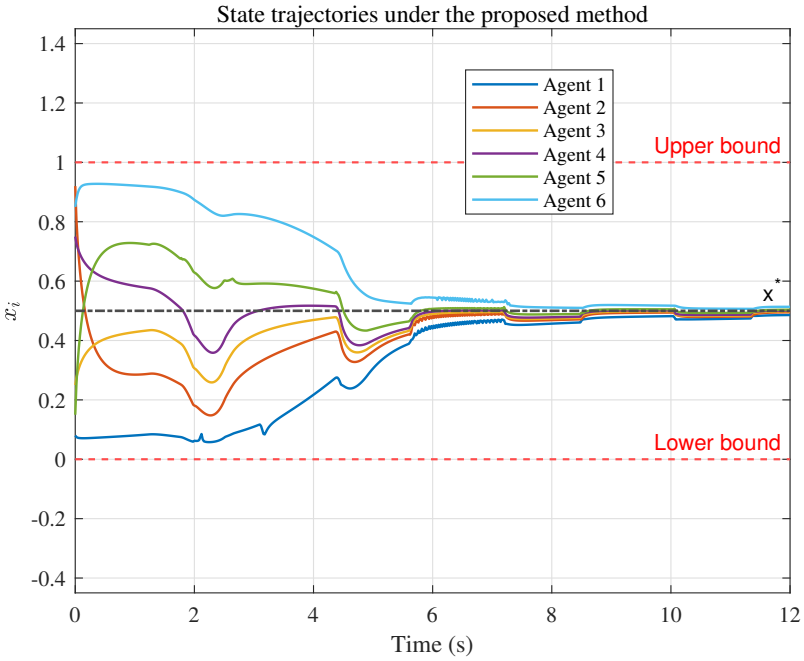


Figure 4. State trajectories under the proposed method.

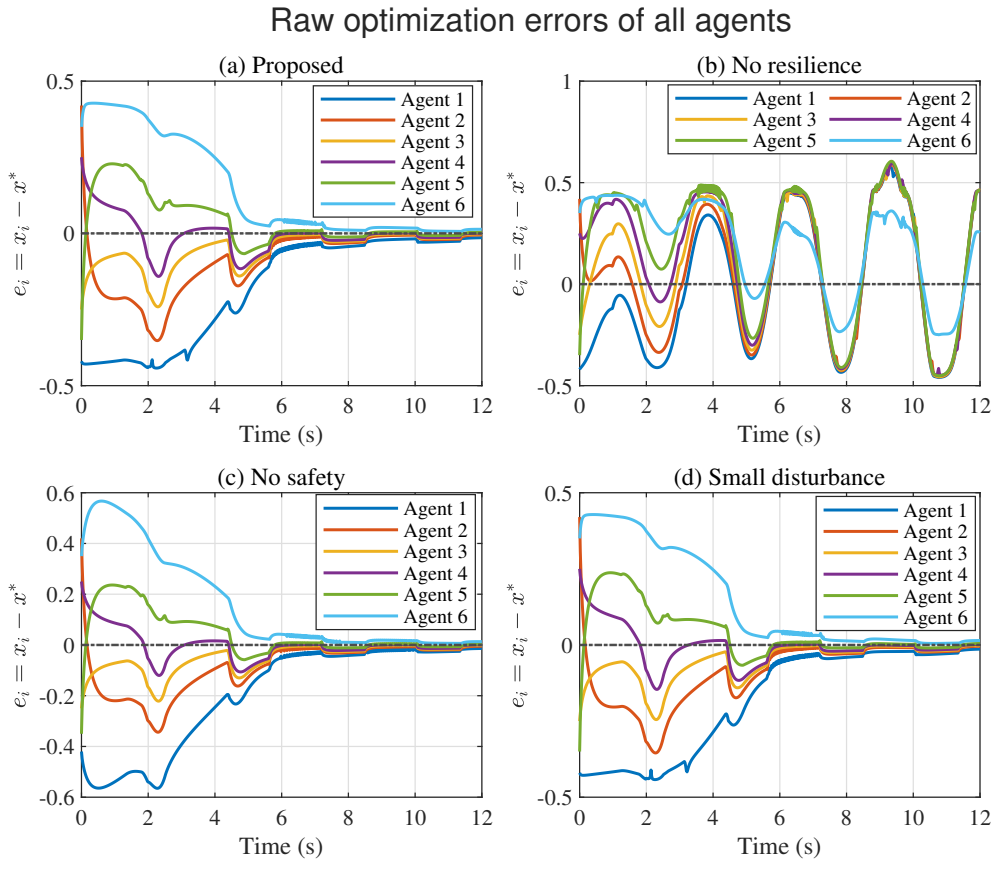


Figure 5. Raw optimization errors under different cases.

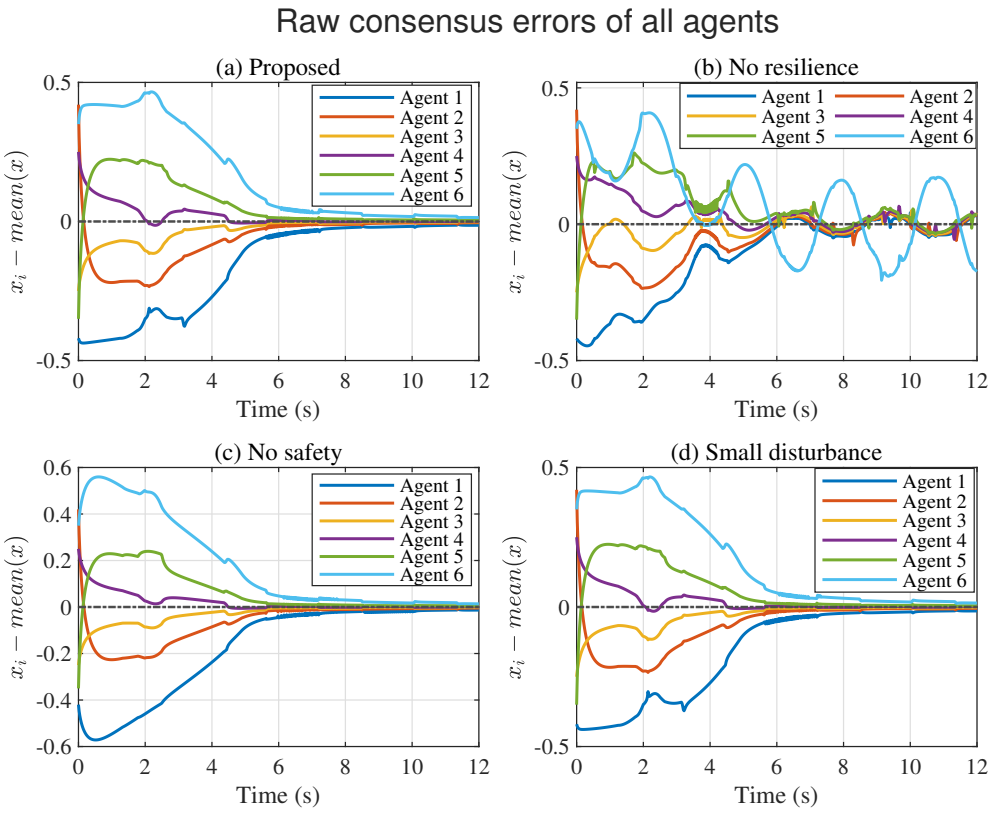


Figure 6. Raw consensus errors under different cases.

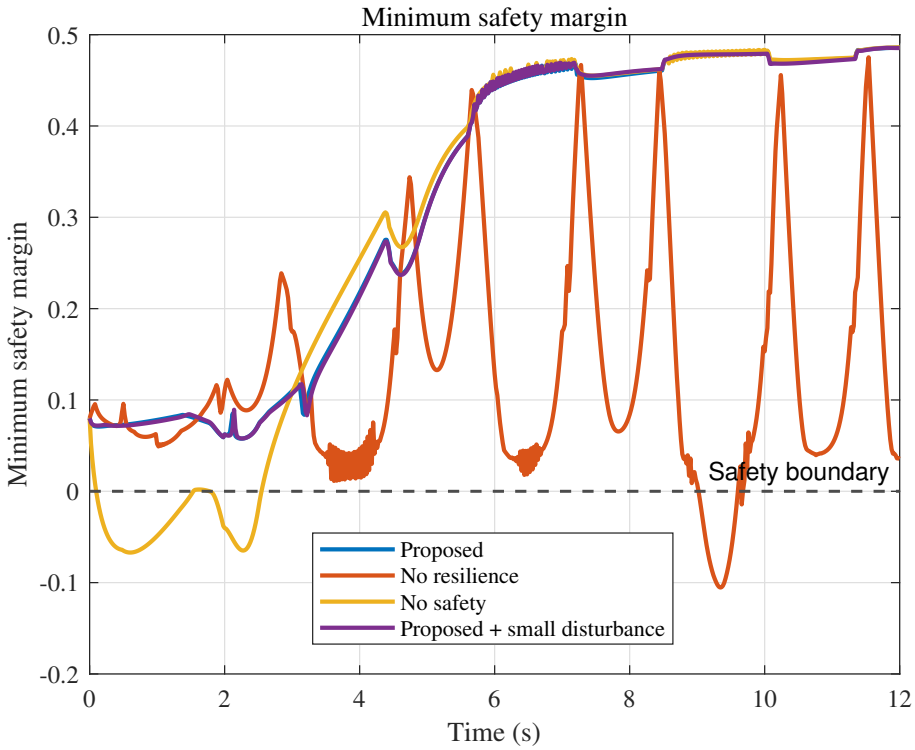


Figure 7. Minimum safety margin under different cases.

Figures 8–10 further illustrate the roles of the resilient processing mechanism and the bounded prescribed-time controller. For clarity, Figure 8 shows one representative channel associated with the attacked transmitter; the local trimming operation reduces the

influence of corrupted neighboring data before the disagreement terms are used by the controller. Figure 9 indicates that the control inputs remain bounded during the whole simulation. Although transient peaks appear due to attack rejection and safety correction, no singular control behavior occurs. Finally, Figure 10 compares the aggregate local cost under different cases. The proposed method remains close to the optimized cost level and avoids the attack-induced oscillatory growth observed in the non-resilient case.

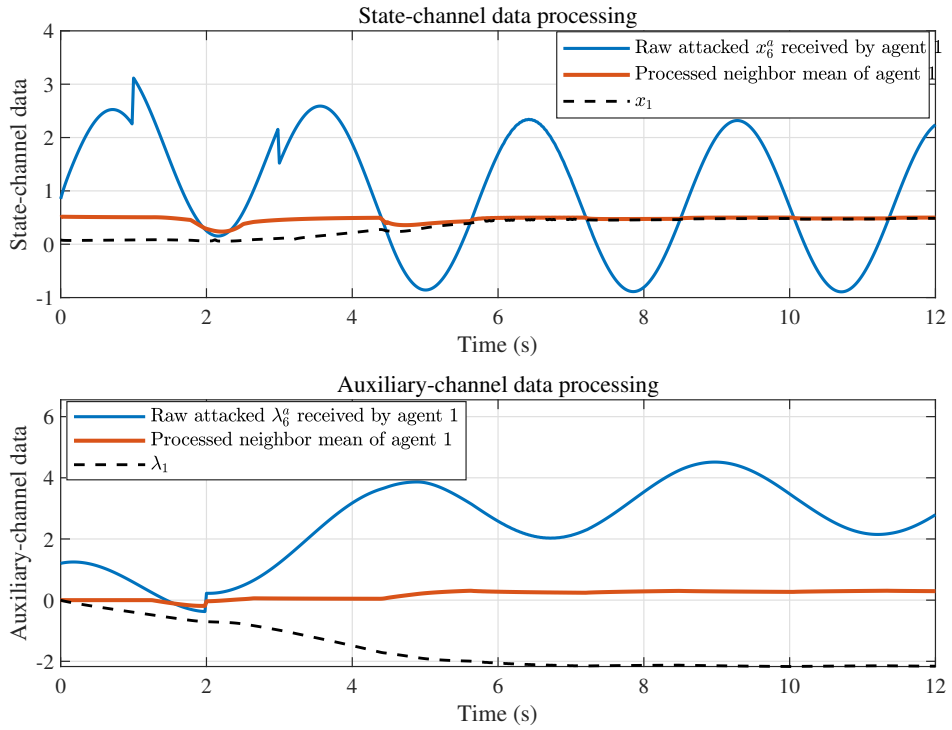


Figure 8. Effect of resilient information processing on corrupted neighboring data.

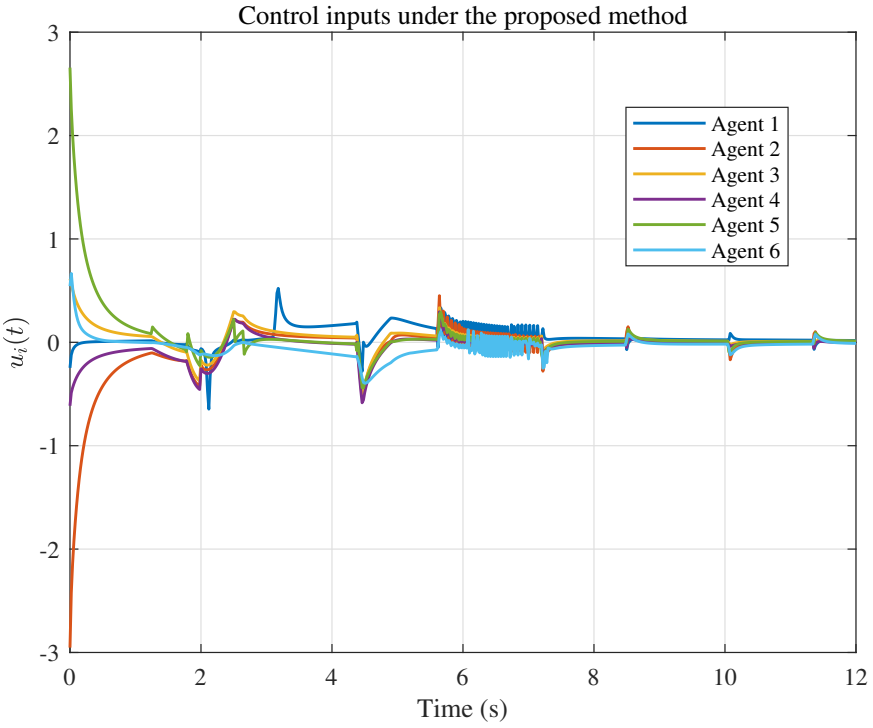


Figure 9. Control inputs under the proposed method.

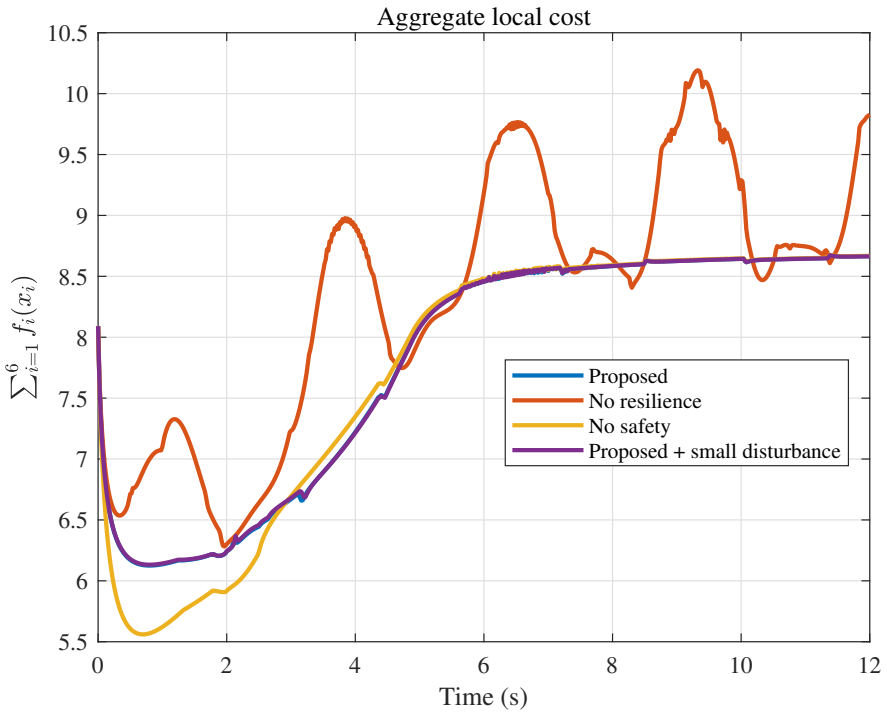


Figure 10. Aggregate local cost under different cases.

Overall, the simulation results support five properties within the tested scenario: approach to a small neighborhood of the optimizer, agreement among normal agents, safety preservation, attenuation of bounded false data injection, and robustness under small disturbances. These observations are consistent with the practical bounds in Theorem 1; they are not presented as proof of performance against arbitrary Byzantine, mobile, or denial-of-service attacks.

8. Discussion

8.1. Interpretation of the Simulation Results

The proposed case achieves a final maximum optimization error of 0.0142, an RMS consensus error of 0.0084, and a positive minimum safety margin of 0.0577. Removing resilient processing increases the final maximum error to 0.4645 and produces 31 unsafe samples. Removing the safety term retains a small final optimization error but produces 111 unsafe samples. These two ablations show that optimization accuracy and transient safety are distinct objectives: a small final cost does not guarantee that the trajectory remained admissible.

The small-disturbance case remains close to the nominal proposed case. This supports the ultimate-boundedness interpretation rather than exact convergence. The bounded control-input plot is also consistent with the use of a saturated prescribed-time gain. Since the simulation uses one topology, one static attacked transmitter, and bounded additive signals, the conclusions are restricted to that setting.

8.2. Comparison with Existing Methods

The comparison in Table 1 shows that the present contribution lies in the intersection of fractional-order dynamics, resilient distributed optimization, state safety, and practical prescribed-time performance. Existing Byzantine-resilient optimization methods [13,14,23] provide stronger adversarial models or multidimensional formulations but do not include the same fractional plant, safety barrier, and assigned-time mechanism. Conversely,

fractional-order and prescribed-time methods [9,19,20] do not address the same communication attack.

A direct numerical transplantation of these algorithms would require changing the agent dynamics, discrete/continuous-time implementation, safety mechanism, attack semantics, and tuning rules. Such a comparison would therefore mix algorithmic performance with model redesign. The revised paper does not claim universal numerical superiority. Instead, the same-model ablations isolate the necessity of the two modules that are central to the proposed design.

8.3. Practical Meaning and Sensitivity of the Threat Bound

The local bound q must be selected from a threat model, network security assessment, or a conservative upper estimate. If the true number of attacked neighbors exceeds the selected value, malicious data may remain after trimming and the residual bounds in (14) no longer apply. The theoretical guarantee is then lost. If q is overestimated while $|\mathcal{N}_i| > 2q$ and Assumption 2 remain valid, more normal data are removed. This does not invalidate the residual bound, but it can reduce $r_{\min}$ and $\underline{\ell}_s$, enlarge the practical error radius, and slow convergence.

The condition $|\mathcal{N}_i| > 2q$ is therefore necessary only for local redundancy; robust post-trimming connectivity is separately required. In applications, q should be chosen together with graph design, authentication mechanisms, and anomaly monitoring. Adaptive estimation of q is an important extension but is not included here because changing q online produces a switched retained graph and requires a new fractional-order analysis.

8.4. Limitations and Future Extensions

The present theorem covers scalar agents, box-type safety in its vector extension, bounded additive communication attacks, and a static locally bounded attacked set. It does not cover unbounded Byzantine messages, mobile attackers, denial-of-service, direct actuator attacks, or arbitrary coupled safe sets. Mobile malicious attacks are particularly nontrivial because the fractional derivative retains the history of nodes that were compromised at earlier times. Addressing that case would require a time-varying threat process and stronger stochastic or switching robustness conditions such as those used in [15,24]. These limitations are stated explicitly so that the contribution is interpreted within its proven scope.

9. Conclusions

This paper developed a resilient safe distributed optimization method with practical prescribed-time performance for fractional-order multi-agent systems under bounded false data injection attacks. The revision provides explicit attack-residual bounds, a checkable gain matrix, a Mittag–Leffler accuracy bound at the assigned time, and a fractional first-hitting proof of safety. The simulations show that resilient filtering and barrier correction play different and necessary roles under the tested static-attack scenario. The method guarantees entrance into an adjustable neighborhood of the global optimizer rather than exact zero-error convergence at T_c. Future work will consider mobile malicious attacks, adaptive threat-bound estimation, directed switching graphs, input constraints, and coupled multidimensional safe sets.

Author Contributions: Conceptualization, C.L. and G.Z.; methodology, C.L., C.Z. and Z.S.; software, C.Z.; formal analysis, C.L., C.Z. and Z.S.; investigation, C.L., C.Z., Y.X. and P.Y.; data curation, C.Z. and P.Y.; writing—original draft preparation, C.L. and C.Z.; writing—review and editing, Z.S. and G.Z.; supervision, Z.S. and G.Z.; funding acquisition, Z.S. and G.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was partly funded by the State Grid Corporation of China Science and Technology Project (J2025059) and Nantong Natural Science Foundation Young Scholars Fund (JC2024039).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The simulation data and code supporting the findings of this study are available from the corresponding author upon reasonable request.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Nedić, A.; Ozdaglar, A. Distributed subgradient methods for multi-agent optimization. *IEEE Trans. Autom. Control* **2009**, *54*, 48–61. [CrossRef]
2. Yang, T.; Yi, X.; Wu, J.; Yuan, Y.; Wu, D.; Meng, Z.; Hong, Y.; Wang, H.; Lin, Z.; Johansson, K.H. A survey of distributed optimization. *Annu. Rev. Control* **2019**, *47*, 278–305. [CrossRef]
3. Wen, G.; Zheng, W.X.; Wan, Y. Distributed robust optimization for networked agent systems with unknown nonlinearities. *IEEE Trans. Autom. Control* **2022**, *68*, 5230–5244. [CrossRef]
4. Braun, P.; Grüne, L.; Kellett, C.M.; Weller, S.R.; Worthmann, K. A distributed optimization algorithm for the predictive control of smart grids. *IEEE Trans. Autom. Control* **2016**, *61*, 3898–3911. [CrossRef]
5. Philip, B.V.; Alpcan, T.; Jin, J.; Palaniswami, M. Distributed real-time IoT for autonomous vehicles. *IEEE Trans. Ind. Inform.* **2018**, *15*, 1131–1140.
6. Podlubny, I. *Fractional Differential Equations: An Introduction to Fractional Derivatives, Fractional Differential Equations, to Methods of Their Solution and Some of Their Applications*; Elsevier: Amsterdam, The Netherlands, 1998; Volume 198.
7. Liu, Y.; Zhang, H.; Shi, Z.; Gao, Z. Neural-network-based finite-time bipartite containment control for fractional-order multi-agent systems. *IEEE Trans. Neural Netw. Learn. Syst.* **2022**, *34*, 7418–7429.
8. Wei, F.; Niu, B.; Zong, G.; Zhao, X. Adaptive neural self-triggered bipartite consensus control for nonlinear fractional-order multi-agent systems with actuator fault. *Nonlinear Dyn.* **2025**, *113*, 729–749.
9. Gong, P.; Wang, Q.-G.; Ahn, C.K. Finite-time distributed optimization in unbalanced multiagent networks: Fractional-order dynamics, disturbance rejection, and chatter avoidance. *IEEE Trans. Autom. Sci. Eng.* **2024**, *22*, 6691–6701.
10. Liu, J.; Zhou, N.; Qin, K.; Chen, B.; Wu, Y.; Choi, K.-S. Distributed optimization for consensus performance of delayed fractional-order double-integrator multi-agent systems. *Neurocomputing* **2023**, *522*, 105–115. [CrossRef]
11. Pasqualetti, F.; Dörfler, F.; Bullo, F. Attack detection and identification in cyber-physical systems. *IEEE Trans. Autom. Control* **2013**, *58*, 2715–2729. [CrossRef]
12. LeBlanc, H.J.; Zhang, H.; Koutsoukos, X.; Sundaram, S. Resilient asymptotic consensus in robust networks. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 766–781. [CrossRef]
13. Zhao, C.; He, J.; Wang, Q.-G. Resilient distributed optimization algorithm against adversarial attacks. *IEEE Trans. Autom. Control* **2020**, *65*, 4308–4315. [CrossRef]
14. Su, L.; Vaidya, N.H. Byzantine-resilient multiagent optimization. *IEEE Trans. Autom. Control* **2021**, *66*, 2227–2233. [CrossRef]
15. Shang, Y. Resilient vector consensus over random dynamic networks under mobile malicious attacks. *Comput. J.* **2024**, *67*, 1076–1086. [CrossRef]
16. Tee, K.P.; Ge, S.S.; Tay, E.H. Barrier Lyapunov functions for the control of output-constrained nonlinear systems. *Automatica* **2009**, *45*, 918–927. [CrossRef]
17. Ames, A.D.; Xu, X.; Grizzle, J.W.; Tabuada, P. Control barrier function based quadratic programs for safety critical systems. *IEEE Trans. Autom. Control* **2016**, *62*, 3861–3876. [CrossRef]
18. Wang, Y.; Song, Y.; Hill, D.J.; Krstić, M. Prescribed-time consensus and containment control of networked multiagent systems. *IEEE Trans. Cybern.* **2018**, *49*, 1138–1147. [CrossRef] [PubMed]
19. Gong, X.; Cui, Y.; Shen, J.; Xiong, J.; Huang, T. Distributed optimization in prescribed-time: Theory and experiment. *IEEE Trans. Netw. Sci. Eng.* **2021**, *9*, 564–576. [CrossRef]
20. Li, H.; Zhang, M.; Yin, Z.; Zhao, Q.; Xi, J.; Zheng, Y. Prescribed-time distributed optimization problem with constraints. *ISA Trans.* **2024**, *148*, 255–263. [CrossRef] [PubMed]
21. Wang, H.; Dong, T.; Yang, Y.; Liu, T.; Wang, A. Singularity-free prescribed-time distributed optimization for nonlinear multi-agent systems with time-varying cost functions. *J. Mach. Learn. Inf. Secur.* **2026**, *2*, 6. [CrossRef]
22. Shang, Y. Resilient consensus of switched multi-agent systems. *Syst. Control Lett.* **2018**, *122*, 12–18. [CrossRef]
23. Kuwaranancharoen, K.; Xin, L.; Sundaram, S. Byzantine-resilient distributed optimization of multi-dimensional functions. In Proceedings of the 2020 American Control Conference, Denver, CO, USA, 1–3 July 2020; pp. 4399–4404. [CrossRef]

24. Wang, Y.; Ishii, H.; Bonnet, F.; Défago, X. Resilient real-valued consensus in spite of mobile malicious agents on directed graphs. *IEEE Trans. Parallel Distrib. Syst.* **2022**, *33*, 586–603. [CrossRef]
25. Li, X.-M.; Zhou, Q.; Li, P.; Li, H.; Lu, R. Event-triggered consensus control for multi-agent systems against false data-injection attacks. *IEEE Trans. Cybern.* **2019**, *50*, 1856–1866. [PubMed]
26. He, W.; Gao, X.; Zhong, W.; Qian, F. Secure impulsive synchronization control of multi-agent systems under deception attacks. *Inf. Sci.* **2018**, *459*, 354–368. [CrossRef]
27. Wu, X.; Ding, S.; Zhao, N.; Wang, H.; Niu, B. Neural-network-based event-triggered adaptive secure fault-tolerant containment control for nonlinear multi-agent systems under denial-of-service attacks. *Neural Netw.* **2025**, *191*, 107725. [CrossRef] [PubMed]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.