Intelligence & Control
https://www.sciltp.com/journals/ic

Article

Privacy-Preserving Model-Free Adaptive Sliding Mode Control for MASs under Dynamic Sparse Attacks

Guangrui Tong, Xiaoyang Liu * and Xiang Jiang

School of Computer Science and Technology, Jiangsu Normal University, Xuzhou 221116, China
* Correspondence: xyliu@jsnu.edu.cn

How To Cite: Tong, G.; Liu, X.; Jiang, X. Privacy-Preserving Model-Free Adaptive Sliding Mode Control for MASs under Dynamic Sparse Attacks. *Intelligence & Control* **2026**, *2*(3), 2. https://doi.org/10.53941/ic.2026.100009

Received: 27 March 2026
Revised: 10 June 2026
Accepted: 7 July 2026
Published: 25 August 2026

Abstract: This paper investigates the data-driven consensus control problem for a class of discrete-time single-input single-output (SISO) nonlinear multi-agent systems(MASs) subject to limited bandwidth resources, dynamic sparse attacks, and communication disturbances. Consensus errors are transmitted over multiple channels, where an attacker can compromise a time-varying subset of these channels. First, to alleviate the communication burden while enhancing resilience, a distributed dynamic event-triggered mechanism (DDETM) is proposed to reduce unnecessary data transmission. Second, an encryption-decryption scheme using multiple symmetric keys is adopted to protect data confidentiality. In conjunction, a data-fusion algorithm is designed to accurately estimate the true output from the corrupted and noisy encrypted data received at triggering instants. Subsequently, a fully distributed model-free adaptive sliding mode control (FDMFASMC) algorithm is developed to ensure the robustness and convergence of the MASs. Finally, a numerical simulation is presented to validate the effectiveness and performance of the proposed control strategy.

Keywords: data-driven control; dynamic sparse attacks; privacy-preserving strategy; event-triggered mechanism; model-free adaptive control; sliding mode control

1. Introduction

In recent years, the cooperative control of multi-agent systems (MASs) has seen extensive application in complex tasks such as vehicle formation, autonomous underwater vehicles, and transportation [1–6]. Various cooperative control frameworks have been established, including leader-following consensus, leaderless consensus, and competitive-cooperative consensus [7–12]. In the widely studied, leader-following consensus, one or more agents act as leaders, guiding the collective behavior of the follower agents. However, despite significant research, most cooperative control strategies depend on accurate system models, which are often difficult or impossible to obtain in practical scenarios due to inherent nonlinearities and unknown dynamics.

To overcome this limitation, data-driven control methods, which design controllers using only system input-output (I/O) data, have emerged as a powerful alternative for MASs with completely unknown dynamics [13–15]. A prominent data-driven approach, is Model-Free Adaptive Control (MFAC), which utilizes a dynamically updated parameter known as the a pseudo-partial derivative (PPD) to construct a compact-form linearized data model of the unknown agent, with the PPD updated adaptively from I/O data online [16]. MFAC algorithms have been successfully applied to consensus tracking problems for unknown MASs subject to various non-ideal conditions, such as faded information [17] and intermittent neighborhood information [18]. While these studies have made significant contributions, they typically operate under the assumption of a secure communication network.

With the advancement of network technologies, the security and privacy of data have become critical concerns [19–23]. For instance, Ref. [24] proposed a resilient MFAC strategy for unknown MASs under denial-of-service (DoS) attacks, and [25] designed an attack-compensation mechanism to handle a class of hybrid-attacks. In [26], a multi-channel data-redundancy scheme was introduced to defend against measurement disturbances and dynamic

sparse attacks, where the adversary can compromise different subsets of sensors over time. Although these studies mitigate the adverse effects of attacks, they provide insufficient protection for data confidentiality during transmission, leaving system information vulnerable to eavesdropping. Intercepted information can enable an attacker to launch more precise and devastating attacks [27]. Therefore, developing effective privacy-preserving mechanisms is essential for the secure operation of networked control. Motivated by these concerns, researchers have explored state-decomposition methods [28], and symmetric-key encryption algorithms [29] to protect privacy in consensus and MFAC strategies.

In parallel, sliding-mode control (SMC) is widely recognized for its exceptional robustness against system uncertainties and external disturbances [30–32]. The integration of SMC with MFAC, known as, model-free adaptive sliding-mode control (MFASMC), combines the advantages of both approaches [33,34]. For instance, Ref. [25] employed an MFASMC scheme to enhance MAS robustness under combined DoS and deception attacks, while Ref. [35] developed a MFASMC with prescribed performance to achieve bipartite consensus tracking. Furthermore, to conserve network resources, Event-Triggered Schemes (ETS) have been extensively studied for model-free MASs, as they reduce communication by transmitting data only when necessary [36–39]. However, achieving secure consensus for model-free MASs that simultaneously addresses cyber-attacks, privacy preservation, and communication efficiency via an integrated ETS and MFASMC framework remains a significant and open challenge.

Motivated by the above considerations, this paper proposes a fully distributed MFASMC strategy incorporating a novel event-triggered-based privacy-preserving mechanism for MASs subject to dynamic sparse attacks. The main contributions are summarized as follows:

(1) Distinct from prior MFAC studies [22–24] that focus solely on attacks, this work considers a more complex scenario where disturbances affect both measurement and communication, and the communication network is subject to dynamic sparse attacks. Under non-ideal communication channels that may induce decryption errors, the errors before encryption and after decryption can be shown to be bounded.

(2) In contrast to previous studies [36,39] that designed event-triggered mechanisms for discrete-time model-free MASs, this paper introduces a distributed dynamic event-triggered mechanism (DDETM) and a data-fusion algorithm to mitigate the impact of sparse attacks on the decryption process. Transmitted data are encrypted only at triggering instants, thereby reducing communication redundancy while preventing information leakage.

(3) A fully distributed model-free sliding-mode control(FDMFASMC) method is developed based on dynamic linearization and a distributed observer, which relies exclusively on local input and output data. Compared with [34, 40], the proposed method is more suitable for large-scale MASs where prior knowledge of the Laplacian matrix is unavailable.

Notations: $\mathbb{R}$ denotes the set of real numbers. $\mathbb{R}^{\kappa}$ is the set of real κ-dimensional vectors. $\mathbb{R}^{n\times n}$ denotes the set of real n-dimensional matrices. $|\cdot|$ is the absolute value notation. $\mathbf{N}^{+}$ means the set of nonnegative integers.

2. Preliminaries and Problem Formulation

2.1. Graph Theory

The communication network of MASs is represented by a weighted graph $\mathfrak{G} \triangleq \{\mathfrak{V}, \mathfrak{E}, \mathfrak{A}\}$, where $\mathfrak{V} = \{1, \ldots, N\}$ denotes the set of follower vertices, $\mathfrak{E} \subseteq \mathfrak{V} \times \mathfrak{V}$ is the set of edges, $\mathfrak{A} = [\alpha_{\imath\jmath}] \in \mathbb{R}^{n\times n}$is the relevant adjacency matrix with $\imath, \jmath \in \mathfrak{V}$. The ordered pair $(\imath, \jmath) \in \mathfrak{E}$ indicates that the agent $\imath$ can receive information from agent $\jmath$, i.e.,$\alpha_{\imath\jmath} = 1$; otherwise,$\alpha_{\imath\jmath} = 0$. $\mathcal{N}_{\imath} = \{\jmath \in \mathfrak{V} | (\imath, \jmath) \in \mathfrak{E}\}$ presents the neighbor collection of agent $\imath$. Define the Laplacian matrix $\mathfrak{L} = [\ell_{\imath\jmath}] \in \mathbb{R}^{n\times n}$ as $\ell_{\imath\imath} = \sum_{\jmath=1,\jmath\neq\imath}^{N} \alpha_{\imath\jmath}$ and $\ell_{\imath\jmath} = -\alpha_{\imath\jmath} (\jmath \neq \imath)$. A variable $\beta_{\imath}$ represents the interaction between the leader 0 and the agent $\imath$, namely, the agent $\imath$ can receive information from the leader if $\beta_{\imath} = 1$; otherwise, $\beta_{\imath} = 0$. A new graph $\bar{\mathfrak{G}} = \{\bar{\mathfrak{V}}, \bar{\mathfrak{E}}, \bar{\mathfrak{A}}\}$, in which $\bar{\mathfrak{V}} = \mathfrak{V} \cup \{0\}$,$\bar{\mathfrak{E}} \subseteq \bar{\mathfrak{V}} \times \bar{\mathfrak{V}}$, and $\bar{\mathfrak{A}}$ is defined to describe the association among N followers and the leader.

2.2. Dynamic Linearization Transformation

Consider the a class of discrete-time SISO nonlinear systems consisting of one leader and N followers. The dynamics of the $\imath$th follower agent is

$$y_{\imath}(k+1) = f_{\imath}(y_{\imath}(k), u_{\imath}(k), \omega_{\imath}(k)), \tag{1}$$

where $y_{\imath}(k), u_{\imath}(k), \omega_{\imath}(k) \in \mathbb{R}$ are the output, input and bounded disturbance at time k, respectively. We assume there exists a positive constant $\bar{\omega}$ such that $|\omega_{\imath}(k)| \leq \bar{\omega}$. The function $f_{\imath}(\cdot)$ represents an unknown nonlinear function.

The leader's trajectory $y_0(k+1)$ is generated by:

$$y_0(k+1) = f_0(y_0(k), u_0(k)), \tag{2}$$

where $f_0(\cdot)$ is also an unknown nonlinear function, and the leader's output $|y_0(k)| \leq b_y$, where $b_y > 0$.

The following standard assumptions are made for the system [18,41,42]:

Assumption 1. *The digraph $\bar{\mathfrak{G}}$ contains a directed spanning tree with the leader as the root.*

Assumption 2. *The partial derivatives of $f_\imath(\cdot)$ with respect to the control input $u_\imath(k)$ are continuous for all $\imath$.*

Assumption 3. *The systems (1) and (2) satisfy the condition: If $|\Delta u_\imath \neq 0|, \imath \in \mathfrak{V}$, there exists a constant $L > 0$, such that*

$$|\Delta y_l(k+1)| \leq L|\Delta u_l(k)|,$$

where $l = 0, 1, \ldots, N$ and $|\Delta d(k+1)| = d(k+1) - d(k), d \in \{y_\imath, u_\imath, y_0, u_0\}$, $L > 0$.

Assumption 4. *The ratio of input changes between any two agents is bounded, i.e., $|\Delta u_\jmath(k)/\Delta u_\imath(k)| \leq \wp$ and $|\Delta u_0(k)/\Delta u_\imath(k)| \leq \wp$ for some positive constant $\wp$ and for all $\imath, \jmath \in \mathfrak{V}$.*

Remark 1. *rem:1 Assumption 1 is a fundamental requirement for achieving the leader-following consensus. Assumption 2 is a standard smoothness condition for nonlinear systems. Assumption 3 is a reasonable property for well-behaved physical systems, ensuring that bounded input changes result in bounded output changes. Assumption 4 is naturally satisfied if the control input increments for all agents are constrained, which is a common practical requirement.*

The distributed consensus error for agent $\imath$ is defined as:

$$\begin{aligned}\zeta_\imath(k+1) = &\sum_{\jmath \in \mathcal{N}_\imath} \alpha_{\imath\jmath}(y_\imath(k+1) - y_\jmath(k+1)) \\ &+ \beta_\imath(y_\imath(k+1) - y_0(k+1)).\end{aligned} \tag{3}$$

Substituting (1) and (2) into (3), the one-step-ahead consensus error $\zeta_\imath(k+1)$ can be expressed as a complex nonlinear function of the states, inputs, and disturbances of agent $\imath$, its neighbors, and the leader. We can write this compactly as:

$$\begin{aligned}\zeta_\imath(k+1) =&\Gamma_\imath[y_\imath(k), u_\imath(k), \omega_\imath(k), y_\jmath(k), u_\jmath(k), \omega_\jmath(k), \\ &y_0(k), u_0(k)].\end{aligned} \tag{4}$$

Lemma 1. *Consider the nonlinear system (1) and (2), under the Assumptions 1–4, and $|\Delta u_\imath(k)| \neq 0$ for all k, the consensus error (3) can be transformed into the following compact linearization model:*

$$\Delta\zeta_\imath(k+1) = \psi_\imath(k)\Delta u_\imath(k) + W_\imath(k), \tag{5}$$

where $\Delta\zeta_\imath(k+1) = \zeta_\imath(k+1) - \zeta_\imath(k)$ and $W_\imath(k)$ is bounded disturbance where $|W_\imath(k)| \leq \bar{W}$. The PPD $\psi_i(k)$ is bounded such that $|\psi_\imath(k)| \leq b_\psi$ with b_ψ being a positive constant.

Proof. From the definition of $\zeta_\imath(k+1)$ in (4), we have:

$$\begin{aligned}&\Delta\zeta_\imath(k+1) \\ &=\Gamma_\imath[y_\imath(k), u_\imath(k), \omega_\imath(k), y_\jmath(k), u_\jmath(k), \omega_\jmath(k), y_0(k), u_0(k)] \\ &\quad - \Gamma_\imath[y_\imath(k), u_\imath(k-1), \omega_\imath(k), y_\jmath(k), u_\jmath(k), \omega_\jmath(k), y_0(k), \\ &\quad u_0(k)] + \Gamma_\imath[y_\imath(k), u_\imath(k-1), \omega_\imath(k), y_\jmath(k), u_\jmath(k), \omega_\jmath(k), \\ &\quad y_0(k), u_0(k)] - \Gamma_\imath[y_\imath(k-1), u_\imath(k-1), \omega_\imath(k-1), \\ &\quad y_\jmath(k-1), u_\jmath(k-1), \omega_\jmath(k-1), y_0(k-1), u_0(k-1)].\end{aligned}$$

Based on Assumption 2, $\Gamma_\imath(\cdot)$ is differentiable with respect to $u_\imath(k)$. Applying the differential mean value theorem yields

$$\Delta\zeta_\imath(k+1) = \frac{\partial\Gamma_\imath^*}{\partial u_\imath(k)}\Delta u_\imath(k) + \Theta_\imath(k),$$

where $\partial\Gamma_\iota^*/\partial u_\iota(k)$ is the value of $\partial\Gamma_\iota/\partial u_\iota(k)$ in the interval between $u_\iota(k-1)$ and $u_\iota(k)$, and

$$\begin{aligned}\Theta_\iota(k) =&\Gamma_\iota\big[y_\iota(k), u_\iota(k-1), \omega_\iota(k), y_\jmath(k), u_\jmath(k), \omega_\jmath(k),\\ &y_0(k), u_0(k)\big] - \Gamma_\iota\big[y_\iota(k-1), u_\iota(k-1),\\ &\omega_\iota(k-1), y_\jmath(k-1), u_\jmath(k-1), \omega_\jmath(k-1),\\ &y_0(k-1), u_0(k-1)\big].\end{aligned}$$

Then, following the approach in [25], the term $\Theta_\iota(k)$ at kth instant can be expressed as

$$\begin{aligned}\Theta_\iota(k) = &\theta_\iota(k)\Delta u_\iota(k) + \sum_{\jmath\in\mathcal{N}_\iota}\alpha_{\iota\jmath}\theta_\jmath(k)\Delta u_\jmath(k)\\ &+ \beta_\iota\theta_0(k)\Delta u_0(k) + \gamma_\iota(k)\Delta\omega_\iota(k)\\ &+ \sum_{\jmath\in\mathcal{N}_\iota}\alpha_{\iota\jmath}\gamma_\jmath(k)\Delta\omega_\jmath(k),\end{aligned}$$

where $\theta_\iota(k), \theta_\jmath(k), \theta_0(k), \gamma_\iota(k), \gamma_\jmath(k)$ are variables.

In view of Assumption 4, $\Theta_\iota(k)$ is transformed into

$$\begin{aligned}\Theta_\iota(k) &= \theta_\iota(k)\Delta u_\iota(k) + \sum_{\jmath\in\mathcal{N}_\iota}\alpha_{\iota\jmath}\theta_\jmath(k)\varsigma_\jmath(k)\Delta u_\iota(k)\\ &\quad + \beta_\iota\theta_0(k)\varsigma_0(k)\Delta u_\iota(k) + W_\iota(k)\\ &= \theta_\iota^*(k)\Delta u_\iota(k) + W_\iota(k),\end{aligned}$$

where $\varsigma_\jmath(k), \varsigma_0(k)$ are variables, $W_\iota(k) = \gamma_\iota(k)\Delta\omega_\iota(k) + \sum_{\jmath\in\mathcal{N}_\iota}\alpha_{\iota\jmath}\gamma_\jmath(k)\Delta\omega_\jmath(k)$ and $\theta_\iota^*(k) = \theta_\iota(k) + \beta_\iota\theta_0(k)\varsigma_0(k) + \sum_{\jmath\in\mathcal{N}_\iota}\alpha_{\iota\jmath}\theta_\jmath(k)\varsigma_\jmath(k)$. Considering the bounded disturbance $|\omega_\iota| \le \bar{\omega}$, it implies $|W_\iota(k)| \le \bar{W}$. Then, Equation (5) follows by choosing $\psi_\iota(k) = \partial\Gamma_\iota^*/\partial u_\iota(k) + \theta_\iota^*(k)$.

Additionally, taking (3) into $\Delta\zeta_\iota(k+1)$, according to Assumptions 3 and 4, one has

$$\begin{aligned}|\Delta\zeta_\iota(k+1)| \le&a_1|\Delta y_\iota(k+1)| + a_2|\Delta y_\jmath(k+1)|\\ &+ \beta_\iota|\Delta y_0(k+1)|\\ \le&(a_1 + a_2\wp + \beta_\iota\wp)L|\Delta u_\iota(k)|\\ \le&(1+\wp)NL|\Delta u_\iota(k)|\\ \triangleq&b_\psi|\Delta u_\iota(k)|,\end{aligned}$$

where $a_1 = \beta_\iota + \sum_{\jmath\in\mathcal{N}_\iota}\alpha_{\iota\jmath}$, $a_2 = \sum_{\jmath\in\mathcal{N}_\iota}\alpha_{\iota\jmath}$ and $b_\psi = (1+\wp)NL$ are positive constants. Combining this with (5) proves that $|\psi_\iota(k)| \le b_\psi$.

The proof is complete. □

2.3. Dynamic Sparse Attacks

Definition 1. *For κ_ι sensors, an attack is called dynamically ς_ι-sparse if the set of compromised channels is allowed to vary over time, while at any instant the adversary can corrupt at most ς_ι of these channels. Here, κ_ι and ς_ι are positive integers with $\kappa_\iota > \varsigma_\iota$.*

For each node, sensor data is transmitted over κ_ι channels. Then, the data transmitted at an event-triggering instant under both ς_ι-sparse attacks and transmission disturbances can be expressed as

$$Y_\iota(k_i) = \iota\breve{\xi}_\iota(k_i) + \varpi_\iota(k_i) + A_\iota(k_i),$$

where $\iota = [1, \ldots, 1]^T \in \mathbb{R}^{\kappa_\iota}$ is the unit column vector, $\breve{\xi}_\iota(k_i), i \in \mathbf{N}^+$ is privacy-protected data at triggering instant k_i, which will be introduced later. $\varpi_\iota(k_i) = [\varpi_{\iota 1}(k_i), \ldots, \varpi_{\iota\kappa_\iota}(k_i)]^T \in \mathbb{R}^{\kappa_\iota}$ is the bounded communication disturbance existing in the channels, and $A_\iota(k_i) = [A_{\iota 1}(k_i), \ldots, A_{\iota\kappa_\iota}(k_i)]^T \in \mathbb{R}^{\kappa_\iota}$ is the dynamic sparse attack vector.

Assumption 5. *The channels' disturbances are bounded. Specifically, there exists a positive constant $\bar{\varpi}$ such that $|\varpi_{\iota o}(k)| \le \bar{\varpi}, o = 1, 2, \ldots, \kappa_\iota$.*

Assumption 6. *For the channel attack vector $A_\imath(k)$,$k \in N^+$, the number of its nonzero components is strictly less than $\kappa_\imath/2$.*

3. Algorithm Design

3.1. DDETM Design

To conserve communication bandwidth and prevent data leakage, a DDETM is proposed. A DDETM determines whether a signal should be transmitted. Once the triggering condition is satisfied, the signal is encrypted and sent over the network in ciphertext. On the controller side, the ciphertext is decrypted. Given the non-ideal communication environment, the decrypted data is further processed by a data-fusion algorithm to generate the output estimates required for secure tracking control.

Denote $h_\imath(k) = \zeta_\imath(k) - \zeta_\imath(k_i)$ as the triggering error, and $\{k_i\}(i = 1, 2, ...)$ is triggering sequence. The triggering instants can be determined as follows:

$$\begin{aligned} k_{i+1} &= \inf\left\{k > k_i \,\middle|\, g_\imath(k) > 0 \ \text{ or } \ k > \bar{k}\right\}, \\ g_\imath(k) &= \rho_\imath|h_\imath(k)| - \nu_\imath - \tfrac{1}{\upsilon_\imath}\hbar_\imath^1(k) - \tfrac{1}{\upsilon_\imath}\hbar_\imath^2(k) \end{aligned} \tag{6}$$

where $\nu_\imath$ is the triggering threshold, $\bar{k}$ is the maximum trigger interval, $\upsilon_\imath$ and $\rho_\imath$ are positive constants. In addition, the internal dynamic variables $\hbar_\imath^1(k)$ and $\hbar_\imath^2(k)$ are defined as

$$\begin{aligned} \hbar_\imath^1(k+1) &= \sigma_\imath\hbar_\imath^1(k) + \nu_\imath - \rho_\imath|h_\imath(k)|, \\ \hbar_\imath^2(k+1) &= \varrho_\imath\hbar_\imath^2(k) - \rho_\imath\frac{2}{\pi}\arctan\big(|h_\imath(k)|\big), \end{aligned}$$

where $\sigma_\imath, \varrho_\imath \in (0, 1)$ are given scales.

3.2. Privacy-Preserving Strategy Design

To safeguard system stability and security, sensitive data must be protected from direct exposure or malicious use. This is achieved through a symmetric encryption scheme employing dual time-varying keys. Therefore, the resulting privacy-preserving strategy for the $\imath$th agent is designed as follows:

$$\begin{cases} \xi_\imath(k_i) = \zeta_\imath(k_i) + G_\imath(k_i), \\ \breve{\xi}_\imath(k_i) = H_\imath(k_i)\xi_\imath(k_i), \end{cases} \tag{7}$$

where $\breve{\xi}_\imath(k_i)$ denotes the encrypted signal to be transmitted, $G_\imath(k_i)$ and $H_\imath(k_i)$ are time-varying symmetric keys with $H_\imath(k_i)$ being nonsingular. Due to disturbances and attacks over the network, the transmitted signal is processed by a data-fusion algorithm, yielding the corresponding received data $\bar{\xi}_\imath(k_i)$. Thus, the decryption algorithm for the $\imath$th agent is designed as follows:

$$\begin{cases} \vec{\xi}_\imath(k_i) = H_\imath^{-1}(k_i)\bar{\xi}_\imath(k_i), \\ \vec{\zeta}_\imath(k_i) = \vec{\xi}_\imath(k_i) - G_\imath(k_i), \end{cases} \tag{8}$$

where $\vec{\zeta}_\imath(k_i)$ denotes the recovered signal by the decryption function.

Remark 2. *To resist cryptanalysis, the keys $G_i(k_i)$ and $H_i(k_i)$ are designed to be time-varying and bounded, with $H_i(k_i)$ nonsingular to ensure decryptability. It is assumed that the transmitter and receiver achieve key synchronization via a pre-shared seed, an authenticated channel, or offline distribution, which is a common requirement in secure communication frameworks [29,42,43]. Under this assumption, the dynamic sparse attacks and network disturbances considered in this paper affect only the transmitted data rather than the key-management mechanism. If key synchronization fails, additional reconstruction errors will occur, and the established privacy and stability guarantees may no longer hold.*

Remark 3. *Note that the data is encrypted and transmitted only at the instant k_i. No transmission occurs during the entire interval $k \in [k_i, k_{i+1})$, until the next triggering condition is met. This mechanism thereby reduces the communication load and alleviates bandwidth usage.*

3.3. Data-Fusion Algorithms Design

Before presenting the algorithms, we introduce the following notation. Let $\mathbf{sort}(Y_\imath(k))$ denote the vector obtained by arranging the entries of $Y_\imath(k)$ in ascending order. The integer $\varsigma_\imath$ specifies the maximum allowable

number of corrupted entries in $Y_\imath(k)$. Under Assumption 6, if the number of channels $\kappa_\imath$ is odd, then $\varsigma_\imath = (\kappa_\imath - 1)/2$; otherwise, $\varsigma_\imath = \kappa_\imath/2 - 1$. Consequently, at least $q_\imath = \kappa_\imath - \varsigma_\imath$ entries of $Y_\imath(k)$ must remain uncorrupted. The functions $\mathbf{median}(\Omega)$ and $\mathbf{mean}(\Omega)$ denote the median and mean of a vector Ω, respectively. Moreover, $\Omega(\beth)$ denotes the $\beth$th entry of Ω, and $\Omega(\beth : \gimel)$ denotes the subvector of Ω consisting of entries from index $\beth$ to $\gimel$.

To mitigate the impact of dynamic sparse attacks, this paper adopts a multi-channel redundancy strategy, whereby identical data are transmitted simultaneously over multiple communication channels. In practice, each channel is inevitably subject to network noise and other disturbances. Accordingly, we develop a data-fusion algorithm to generate the output estimates required for secure tracking control in the presence of dynamic sparse attacks.

Given the known disturbance upper bound $\bar{\varpi}$, Data-Fusion Algorithm 1 is designed. The algorithm first utilizes $\bar{\varpi}$ to identify and discard corrupted data, and subsequently computes the final output estimate. Its detailed procedure is outlined in Algorithm 1, and its performance is formally established in Proposition 1.

Algorithm 1 Data-Fusion Output Estimation With Known $\bar{\varpi}$

Input: $Y_\imath(k_i)$; $\kappa_\imath$;$\varsigma_\imath$; $\bar{\varpi}$
Output: $\bar{\xi}_\imath(k_i)$; $\bar{\Omega}$

```
Initialize η_ı := κ_ı; Ω := sort(Y_ı(k_i)); q_ı := κ_ı − ς_ı
while Ω(q_ı) − Ω(1) > 2ϖ̄ do
    Ω := Ω(2 : η_ı); η_ı := η_ı − 1
end while
while Ω(η_ı) − Ω(η_ı − q_ı + 1) > 2ϖ̄ do
    Ω := Ω(1 : η_ı − 1); η_ı := η_ı − 1
end while
Ω̄ := Ω
if η_ı > q_ı then
    ξ̄_ı(k_i) := median(Ω̄)
else
    ξ̄_ı(k_i) := mean(Ω̄)
end if
```

Proposition 1. *Consider the transmitted data $Y_\imath(k_i)$, $i \in \mathbf{N}^+$, which are subject to disturbances and dynamic sparse attacks under Assumption 5 and 6. For Algorithm 1 with known disturbance bound $\bar{\varpi}$, the fused outputs $\bar{\xi}_\imath(k_i)$ satisfy $|\bar{\xi}_\imath(k_i) - \xi_\imath(k_i)| \leq \bar{\varpi}$ [29].*

Remark 4. *The performance guarantee of Algorithm 1 relies on a valid upper bound $\bar{\varpi}$of channel disturbances. If the actual disturbances satisfy $\varpi_{\imath\kappa_\imath}(k_i) \leq \bar{\varpi}$, the fused output $\bar{\xi}_\imath(k_i)$ remains bounded, and the error bound in Proposition 1 can be guaranteed. An overestimated $\bar{\varpi}$ only leads to a more conservative fusion error bound and may enlarge the ultimate tracking error bound. However, if $\varpi_{\imath\kappa_\imath}(k_i) > \bar{\varpi}$, some normal channel data may be mistakenly discarded, and the bound in Proposition 1 may no longer hold. Therefore, $\bar{\varpi}$ should be selected as a conservative upper bound in practice.*

3.4. The Fully Distributed MFASMC Algorithm Design

In practice, it is challenging to obtain the true value of the PPD parameter $\psi_\imath(k)$. To address this issue, the following estimation law based on DDETM is employed to update its estimate:

$$\begin{aligned}\mathcal{J}_\imath(\hat{\psi}_\imath(k)) = &|\Delta\vec{\zeta}_\imath(k_i) - \hat{\psi}_\imath(k)\Delta u_\imath(k-1)|^2 \\ &+ \delta_\imath|\hat{\psi}_\imath(k) - \hat{\psi}_\imath(k-1)|^2.\end{aligned} \tag{9}$$

where $\Delta\vec{\zeta}_\imath(k_i) = \vec{\zeta}_\imath(k_i) - \vec{\zeta}_\imath(k_{i-1})$, $\hat{\psi}_\imath(k)$ is the estimate of the PPD parameter $\psi_\imath(k)$, $\delta_\imath$ is given positive constant. By setting the derivative of $\mathcal{J}_\imath(\hat{\psi}_\imath(k))$ with respect to $\hat{\psi}_\imath(k)$ to zero, the update algorithm for $\hat{\psi}_\imath(k)$ is obtained as follows:

$$\begin{aligned}\hat{\psi}_\imath(k) = \hat{\psi}_\imath(k-1) &+ \frac{\epsilon_\imath\Delta\vec{\zeta}_\imath(k_i)\Delta u_\imath(k-1)}{\Delta u_\imath^2(k-1) + \delta_\imath} \\ &- \frac{\epsilon_\imath\hat{\psi}_\imath(k-1)\Delta u_\imath^2(k-1)}{\Delta u_\imath^2(k-1) + \delta_\imath},\end{aligned} \tag{10}$$

where $\epsilon_\imath$ is a step-size factor. To enhance the reliability of (10), a reset algorithm for $\hat{\psi}_\imath(k)$ is introduced as follows:

$$\hat{\psi}_\imath(k) = \hat{\psi}_\imath(1), \text{if } |\hat{\psi}_\imath(k)| \leq p_\imath \text{ or } |\Delta u_\imath(k-1)| \leq p_\imath,$$

where $\hat{\psi}_\imath(1) > p_\imath$ is the initial value of $\hat{\psi}_\imath(k)$ and $p_\imath$ is a small positive constant which is frequently chosen as 10^{-5} [18].

The sliding function of agent $\imath$ is designed as

$$s_\imath(k) = \zeta_\imath(k). \tag{11}$$

The reaching law of agent $\imath$ is designed as follows:

$$s_\imath(k+1) = (1 - z_1 T)s_\imath(k) - z_2 T\tanh(s_\imath(k)), \tag{12}$$

where z_1 and z_2 are positive constants, and T is the discrete-time sample period with $1 - z_1 T > 0$. Combining (11) and (12), it can be obtained

$$\zeta_\imath(k+1) = (1 - z_1 T)s_\imath(k) - z_2\tanh(s_\imath(k)).$$

Since $\zeta_\imath(k+1)$ is unmeasurable time k, the following observer can be constructed to cope with this difficulty

$$\hat{\zeta}_\imath(k+1) = \hat{\zeta}_\imath(k) + \hat{\psi}_\imath(k)\Delta u_\imath(k) + E_\imath(\vec{\zeta}_\imath(k_i) - \hat{\zeta}_\imath(k)), \tag{13}$$

where $\hat{\zeta}_\imath(k)$ is the estimate of the consensus error $\zeta_\imath(k)$ and $E_\imath$ denotes the observer gain.

Then, combined with decryption algorithm (8), the control law can be described as follows:

$$\begin{cases} \varepsilon_\imath(k) = -z_1 T\hat{\psi}_\imath^{-1}(k)\vec{\zeta}_\imath(k_i) + (1 - E_\imath)\hat{\psi}_\imath^{-1}(k)(\vec{\zeta}_\imath(k_i) \\ \qquad\qquad - \hat{\zeta}_\imath(k)) - z_2 T\hat{\psi}_\imath^{-1}(k)\tanh(\vec{\zeta}_\imath(k_i)), \\ u_\imath(k) = \begin{cases} u_\imath(k-1) + \mu\text{sign}(\varepsilon_\imath(k)), & |\varepsilon_\imath(k)| > \mu, \\ u_\imath(k-1) + \varepsilon_\imath(k), & |\varepsilon_\imath(k)| \le \mu, \end{cases} \end{cases} \tag{14}$$

where μ is an adjustable parameter introduced to prevent overly rapid variations in the control input $u_\imath(k)$ from destabilizing the system [35].

Remark 5. *It worth noting that the design of* (3)*,* (9)*,* (10) *and* (11)*–*(14) *relies exclusively on local neighbor information, without requiring any knowledge of the global Laplacian matrix or its eigenvalues. This renders the proposed MFASMC scheme fully distributed, making it more suitable for large-scale MASs where the global network topology information is unavailable.*

Remark 6. *Compared with the existing results, the proposed fully distributed MFASMC strategy incorporating an event-triggered privacy-preserving mechanism has the following distinct advantages. (1).Relative to the MFAC studies in [22–24], this paper considers a more challenging communication environment where measurement disturbances, communication disturbances, and dynamic sparse attacks coexist; (2).Unlike the ETM adopted in [36, 39], the proposed DDETM with a data-fusion algorithm to reconstruct reliable transmitted signals from redundant channels, thereby reducing the influence of sparse attacks and channel disturbances; (3).In contrast to the MFAC algorithms in [34] and [40], the proposed MFASMC framework is fully distributed and does not require prior knowledge of the Laplacian matrix. Thus, each agent can implement the controller using only local information, which improves its applicability to unknown nonlinear multi-agent systems with uncertain communication topology.*

4. Convergence Analysis

Theorem 1. *Consider MASs* (1) *and* (2) *subject to dynamic sparse attacks and bounded unknown disturbances, the FDMFASMC algorithm* (9)*-*(14) *guarantees that the consensus error is ultimately uniformly bounded (UUB), provided that Assumptions 1-6 and* $|H_\imath^{-1}(k_i)| \le \bar{H}$*,* $\bar{H} > 0$*,* $E_\imath \in [0, 1)$*,* $\epsilon_\imath \in (0, 1]$*,* $\delta_\imath > 0$*,* $z_2 > 0$*,* $T > 0$*,* $1 - z_2 T > 0$*.*

Proof. Part I: Demonstrates the boundedness of the decryption error $e_{1,\imath}(k_i) = \zeta_\imath(k_i) - \vec{\zeta}_\imath(k_i)$.

Under the DDETM (6), measurement data are transmitted exclusively at triggering instants. Combined with the data-fusion algorithm, the data received by the controller at those instants can be expressed as

$$\bar{\xi}_\imath(k_i) = \breve{\xi}_\imath(k_i) + \lambda_\imath(k_i). \tag{15}$$

According to Proposition 1, $\lambda_i(k_i)$ remains bounded [26]. For clarity, let $|\lambda_i(k_i)| \leq \bar{\lambda}$. By combining (15) with encryption-decryption algorithms (7), (8) and taking the absolute value of $e_{1,i}(k_i)$, it is clear that

$$\begin{aligned}|e_{1,i}(k_i)| &= \left|\zeta_i(k_i) - \vec{\zeta}_i(k_i)\right| \\ &= \left|\zeta_i(k_i) - [H_i^{-1}(k_i)(\breve{\xi}_i(k_i) + \lambda_i(k_i)) - G_i(k_i)]\right| \\ &= \left|H_i^{-1}(k_i)\lambda_i(k_i)\right| \leq \bar{\lambda}\bar{H} \triangleq \Lambda_1,\end{aligned}$$

which indicates that transmission error $e_{1,i}(k_i)$ is bounded.

Part II: Establishes the boundedness of the increment $\Delta\vec{\zeta}_i(k_i) = \vec{\zeta}_i(k_i) - \vec{\zeta}_i(k_{i-1})$.

According to Lemma 1, encryption-decryption algorithms (7), (8), and control law (14), it has

$$\begin{aligned}|\Delta\vec{\zeta}_i(k_i)| &= \left|\vec{\zeta}_i(k_i) - \vec{\zeta}_i(k_{i-1})\right| \\ &= \left|\zeta_i(k_i) - \zeta_i(k_{i-1}) + H_i^{-1}(k_i)\lambda_i(k_i)\right. \\ &\quad \left. - H_i^{-1}(k_{i-1})\lambda_i(k_{i-1})\right| \\ &\leq \left|\zeta_i(k_i) - \zeta_i(k_i - 1) + \cdots + \zeta_i(k_{i-1} + 1)\right. \\ &\quad \left. - \zeta_i(k_{i-1})\right| + 2\Lambda_1 \\ &\leq \bar{k}b_\psi\mu + 2\Lambda_1 \triangleq \Lambda_2,\end{aligned}$$

which implies that $\Delta\vec{\zeta}_i(k_i)$ is uniformly bounded.

Part III: Analyzes the stability of the PPD estimation error $\tilde{\psi}_i(k) = \psi_i(k) - \hat{\psi}_i(k)$.

Take the absolute value of PPD estimation (10), it yields,

$$\begin{aligned}|\tilde{\psi}_i(k)| = \Big|&\psi_i(k) - \psi_i(k-1) + \psi_i(k-1) - \hat{\psi}_i(k-1) \\ &- \frac{\epsilon_i\,\Delta\vec{\zeta}_i(k_i)\,\Delta u_i(k-1)}{\Delta u_i^2(k-1) + \delta_i} \\ &+ \frac{\epsilon_i\big[\psi_i(k-1) - \tilde{\psi}_i(k-1)\big]\Delta u_i^2(k-1)}{\Delta u_i^2(k-1) + \delta_i}\Big| \\ \leq &\left|1 - \frac{\epsilon_i\,\hat{\psi}_i(k-1)\,\Delta u_i^2(k-1)}{\Delta u_i^2(k-1) + \delta_i}\right| |\tilde{\psi}_i(k-1)| \\ &+ |\Delta\psi_i(k)| + \left|\frac{\epsilon_i\,\psi_i(k-1)\,\Delta u_i^2(k-1)}{\Delta u_i^2(k-1) + \delta_i}\right| \\ &+ \frac{\epsilon_i\,|\Delta\vec{\zeta}_i(k_i)|\,|\Delta u_i(k-1)|}{|\Delta u_i^2(k-1) + \delta_i|},\end{aligned}$$

where $\Delta\psi_i(k) = \psi_i(k) - \psi_i(k-1)$. According to Lemma 1, it can be obtained that $|\Delta\psi_i(k)| \leq 2b_\psi$.

As the function $\frac{\epsilon_i\Delta u_i^2(k-1)}{\Delta u_i^2(k-1)+\delta_i}$ is monotonically increasing with respect to $\Delta u_i^2(k-1)$, its maximum and minimum value are $\frac{\epsilon_i\mu^2}{\mu^2+\delta_i}$ and $\frac{\epsilon_i p_l^2}{p_l^2+\delta_i}$, respectively. Hence, $|1 - \frac{\epsilon_i\hat{\psi}_i(k-1)\Delta u_i^2(k-1)}{\Delta u_i^2(k-1)+\delta_i}|$ is a monotonically decreasing function for $\Delta u_i^2(k-1)$, it holds with $\epsilon_i \in (0, 1]$ and $\delta_i > 0$ that

$$0 < |1 - \frac{\epsilon_i\hat{\psi}_i(k-1)\Delta u_i^2(k-1)}{\Delta u_i^2(k-1) + \delta_i}| \leq \aleph_1 < 1.$$

Furthermore, it is clear that the function $\frac{\epsilon_i|\Delta u_i(k-1)|}{|\Delta u_i^2(k-1)+\delta_i|}$ first increases and then decreases with respect to the variable $\Delta u_i(k-1)$ and attains its maximum value $\frac{1}{2\sqrt{\delta_i}}$ when $\Delta u_i(k-1) = \sqrt{\delta_i}$.

From the above analysis, it can be concluded that

$$\begin{aligned}|\tilde{\psi}_i(k)| &\leq \aleph_1\,|\tilde{\psi}_i(k-1)| + \aleph_2 \\ &\leq \aleph_1\left|\aleph_1\tilde{\psi}_i(k-2) + \aleph_2\right| + \aleph_2 \\ &\leq \aleph_1^{k-1}\tilde{\psi}_i(1) + \aleph_2\,\frac{(1-\aleph_1)^{k-1}}{1-\aleph_1} \triangleq \Lambda_3,\end{aligned}$$

where $\aleph_2 = 2b_\psi + |\frac{\epsilon_i b_\psi\mu^2}{\mu^2+\delta_i}| + |\frac{\epsilon_i\Lambda_2}{2\sqrt{\delta_i}}|$, and $\tilde{\psi}_i(k)$ is uniformly bounded.

Part IV: Proves the boundedness of the observer error $e_{2,\imath}(k+1) = \zeta_\imath(k+1) - \hat{\zeta}_\imath(k+1)$.

Combining (5) and (13), it can be derived that

$$\begin{aligned} e_{2,\imath}(k+1) &= e_{2,\imath}(k) - \tilde{\psi}_\imath(k)\Delta u_\imath(k) + W_\imath(k) - E_\imath\big(\vec{\zeta}_\imath(k_i) \\ &\quad - \hat{\zeta}_\imath(k) + \zeta_\imath(k) - \zeta_\imath(k) - h_\imath(k) + h_\imath(k)\big) \\ &= (1 - E_\imath)e_{2,\imath}(k) - \tilde{\psi}_\imath(k)\Delta u_\imath(k) \\ &\quad - E_\imath\big(\vec{\zeta}_\imath(k_i) - \zeta_\imath(k_i) - h_\imath(k)\big) + W_\imath(k) \\ &= (1 - E_\imath)e_{2,\imath}(k) - \tilde{\psi}_\imath(k)\Delta u_\imath(k) \\ &\quad + E_\imath e_{1,\imath}(k_i) + E_\imath h_\imath(k) + W_\imath(k), \end{aligned} \tag{16}$$

where $h_\imath(k) = \zeta_\imath(k) - \zeta_\imath(k_i)$. Then, taking the absolute value for (16), it has

$$\begin{aligned} |e_{2,\imath}(k+1)| &\le |1 - E_\imath|\,|e_{2,\imath}(k)| + \Lambda_3\mu + E_\imath\Lambda_1 + E_\imath\bar{k}b_\psi\mu \\ &\le \aleph_3^k\,\big|e_{2,\imath}(1)\big| + \aleph_4\,\frac{1 - \aleph_3^k}{1 - \aleph_3} \triangleq \Lambda_4, \end{aligned}$$

where $\aleph_3 = |1 - E_\imath|$ and $\aleph_4 = \Lambda_3\mu + E_\imath\Lambda_1 + E_\imath\bar{k}b_\psi\mu + \bar{W}$. This indicates that $|e_{2,\imath}(k+1)|$ is uniformly bounded.

Part V: Concludes the UUB property of the global consensus error $\zeta_\imath(k)$.

Let $\phi_\imath(k) = \frac{\Delta u_\imath(k)}{\varepsilon_\imath(k)}$ with $\phi_\imath(k) \in (0, 1]$, and taking (14) into (13), it can be derived that

$$\begin{aligned} \hat{\zeta}_\imath(k+1) &= \hat{\zeta}_\imath(k) + \hat{\psi}_\imath(k)\,\phi_\imath(k)\,\varepsilon_\imath(k) + E_\imath\big(\vec{\zeta}_\imath(k_i) - \hat{\zeta}_\imath(k)\big) \\ &= \hat{\zeta}_\imath(k) + E_\imath\big(\vec{\zeta}_\imath(k_i) - \hat{\zeta}_\imath(k)\big) + \phi_\imath(k) \\ &\quad \times \Big[-z_1 T\,\vec{\zeta}_\imath(k_i) + (1 - E_\imath)\big(\vec{\zeta}_\imath(k_i) - \hat{\zeta}_\imath(k)\big) \\ &\quad - z_2 T\tanh\big(\vec{\zeta}_\imath(k_i)\big)\Big] \\ &= \big(1 - z_1 T\,\phi_\imath(k)\big)\hat{\zeta}_\imath(k) - z_2 T\,\tanh\big(\vec{\zeta}_\imath(k_i)\big) \\ &\quad + \big[E_\imath + (1 - E_\imath)\phi_\imath(k) - z_1 T\,\phi_\imath(k)\big] \\ &\quad \times \big(\vec{\zeta}_\imath(k_i) - \hat{\zeta}_\imath(k)\big). \end{aligned}$$

Take the absolute value of $\vec{\zeta}_\imath(k_i) - \hat{\zeta}_\imath(k)$, it has

$$\begin{aligned} &|\vec{\zeta}_\imath(k_i) - \hat{\zeta}_\imath(k)| \\ &\quad = \big|\vec{\zeta}_\imath(k_i) - \zeta_\imath(k_i) + \zeta_\imath(k_i) - \zeta_\imath(k) + \zeta_\imath(k) - \hat{\zeta}_\imath(k)\big| \\ &\quad \le |e_{1,\imath}(k_i)| + |e_{2,\imath}(k_i)| + \bar{k}b_\psi\mu \triangleq \Lambda_5. \end{aligned}$$

Due to $\phi_\imath(k) \in (0, 1]$ and $1 - z_1 T > 0$, one has

$$0 < |1 - z_1 T\phi_\imath(k)| < \aleph_5 < 1.$$

Then, it can be deduced that

$$\begin{aligned} |\hat{\zeta}_\imath(k+1)| &\le \aleph_5\,|\hat{\zeta}_\imath(k)| + \aleph_6 \\ &\le \aleph_5^2\,|\hat{\zeta}_\imath(k-1)| + \aleph_5\aleph_6 + \aleph_6 \\ &\le \cdots \le \aleph_5^k\,|\hat{\zeta}_\imath(1)| + \aleph_6\frac{1 - \aleph_5^k}{1 - \aleph_5} \triangleq \Lambda_6, \end{aligned}$$

where $\aleph_6 = \Lambda_5(\max\{E_\imath, 1 - z_1 T\} + z_2 T)$ and $|\hat{\zeta}_\imath(k+1)|$ is is bounded.

According to the above analysis, it can be obtained that

$$|\zeta_\imath(k)| \le |\hat{\zeta}_\imath(k)| + |e_{2,\imath}(k)| \le \Lambda_4 + \Lambda_6 \triangleq \Lambda_7.$$

Therefore, $\zeta_\imath(k)$ is ultimately uniformly bounded.

The proof is thus complete. □

5. Simulation and Experiments

To verify the theoretical findings, a MAS consisting of one leader and seven followers is considered, in which the dynamics are formulated as

$$\begin{cases} y_1(k+1) = u_1(k) + \dfrac{y_1(k)}{1+y_1^2(k)}, \\ y_2(k+1) = 0.4sin(y_2(k)) + 0.8u_2(k), \\ y_3(k+1) = 0.9u_3(k) + 0.5\dfrac{y_3^3(k)}{1+y_3^4(k)}, \\ y_4(k+1) = 0.6cos(y_4(k)) + 0.7u_4(k), \\ y_5(k+1) = u_5(k) + 0.8cos(y_5(k)) - 0.5sin(y_5(k)), \\ y_6(k+1) = -0.6sin(y_2(k)) + 0.6u_6(k), \\ y_7(k+1) = -0.5cos(y_7(k)) + 0.5u_7(k). \end{cases}$$

Consider the following desired trajectory:

$$y_0(k) = \begin{cases} -5 - 3sin(\dfrac{\pi}{250}), & 0 < k < 700, \\ 103, & k > 700. \end{cases}$$

Figure 1 illustrates the topology graph, which contains a directed spanning tree rooted at the leader. In this simulation, the controlled system parameters and initial conditions are as follows: $y_1(1) = 15, y_2(1) = -25, y_3(1) = -32, y_4(1) = 10, y_5(1) = 2.1, y_6(1) = 8, y_7(1) = 3$, $u_1(1) = u_2(1) = \cdots = u_7(1) = 0.1$, $\kappa_\imath = 7$, $\upsilon_\imath = 200$, $\rho_\imath = 30$, $\nu_1 = 100$, $\nu_2 = 20$, $\nu_3 = 100$, $\nu_4 = 20$, $\nu_5 = 100$, $\nu_6 = 20$, $\nu_7 = 50$, $\sigma_\imath = 0.95$, $\varrho_\imath = 0.5$, $\epsilon_\imath = 1.11$, $\delta_\imath = 20.2$, $p_\imath = 10^{-5}$, $E_\imath = 0.935$, $z_1 = 2.3$, $z_2 = 0.1$, $T = 0.005$, $\mu = 0.8$. Measurement disturbances of each agent are $\omega_1(k) = 0.1sin(\frac{\pi}{k})$, $\omega_2(k) = 0.2cos(\frac{\pi}{k})$, $\omega_3(k) = 0.3sin(\frac{\pi}{k})$, $\omega_4(k) = 0.15sin(\frac{\pi}{k})$, $\omega_5(k) = 0.25cos(\frac{\pi}{k})$, $\omega_6(k) = 0.5cos(\frac{\pi}{k})$, $\omega_7(k) = 0.2sin(\frac{\pi}{k})$. The number of channels is seven, and communication disturbances are uniform random disturbances, namely $\varpi_\imath(k) = \mathcal{U} \sim (-2, 2)$. In addition, dynamic sparse attacks are bounded and uniformly distributed over (−10,10), i.e., $A_{\imath\kappa_\imath}(k_i) \sim (-10, 10)$, and are zero for unattacked channels.

Figure 2 illustrates the tracking performance, confirming that all followers successfully track the target trajectory despite sudden changes at $k = 700$. In addition, the dynamic sparse attacks in the transmission channels of agent $\imath$ is shown in Figure 3.

As illustrated in Figure 4, the seven agents with the DDETM exhibit a notable reduction in information transmission frequency.

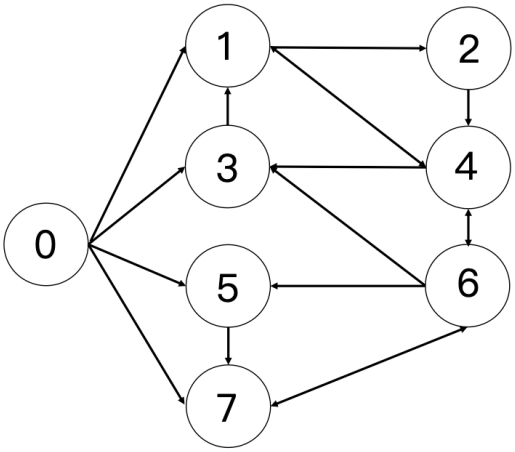

Figure 1. Communication topology $\mathfrak{G}$.

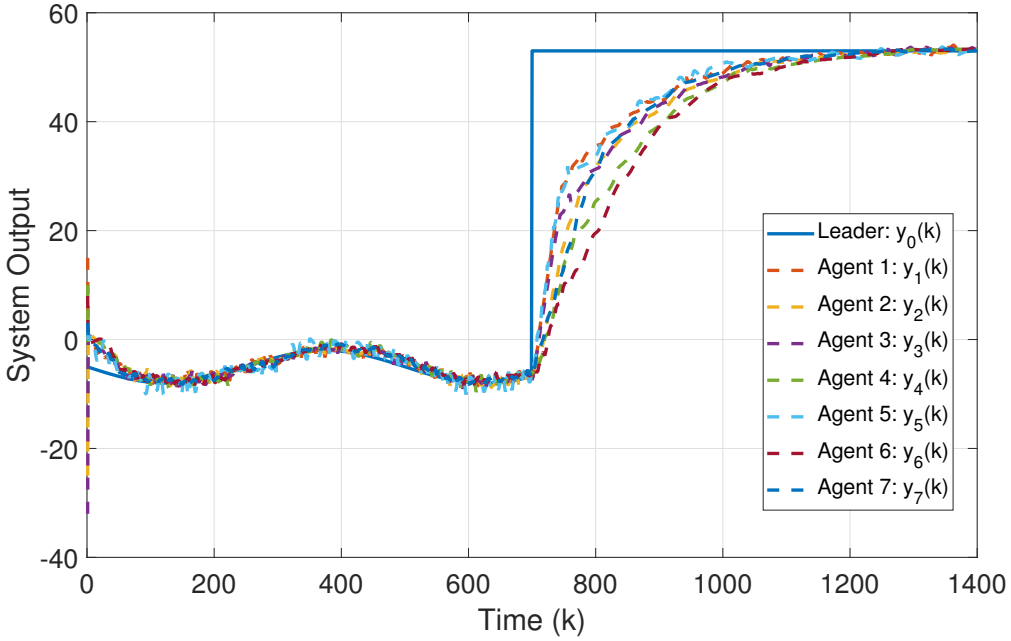

Figure 2. Tracking performance of each agent i.

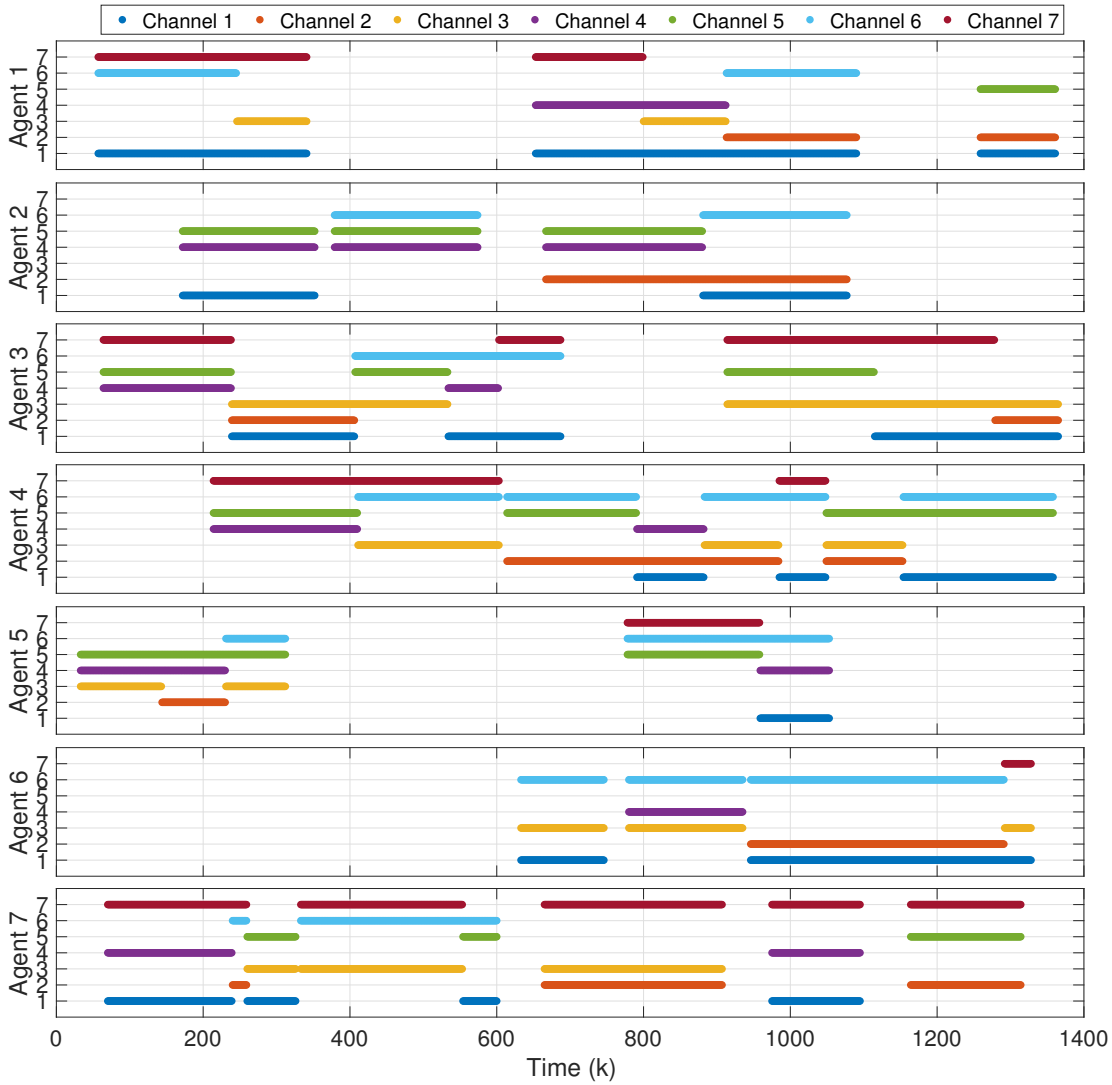

Figure 3. Dynamic sparse attacks on multi-channels.

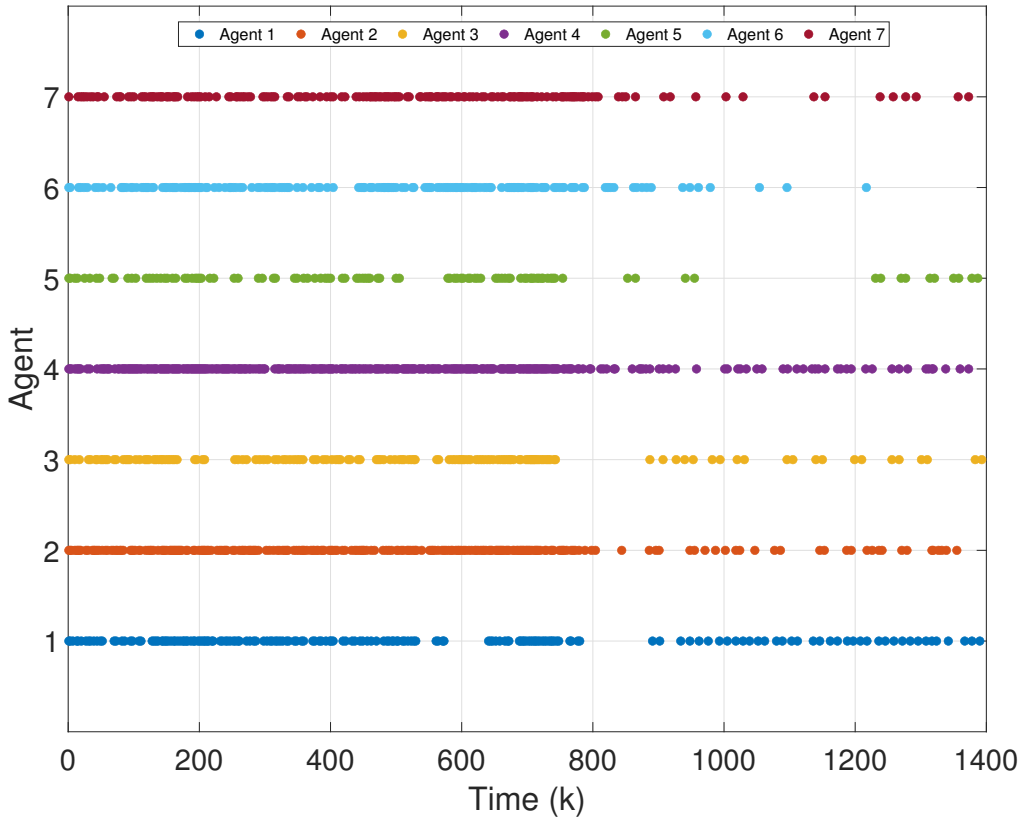

Figure 4. The triggering instants of agent $\imath$.

Figure 5 reveals that both tracking errors $(e_\imath(k) = y_\imath(k) - y_0(k), \imath = 1, 2, ..., 7)$ and consensus errors $\zeta_\imath(k)$ converge to a small neighborhood of the origin, which confirms the robustness of the FDMFASMC algorithm against dynamic sparse attacks (illustrated in Figure 3) and channel disturbances. These results demonstrate that, even in the presence of such attacks and uncertainties, the proposed scheme ensures bounded convergence of both tracking and consensus errors, thereby verifying its effectiveness.

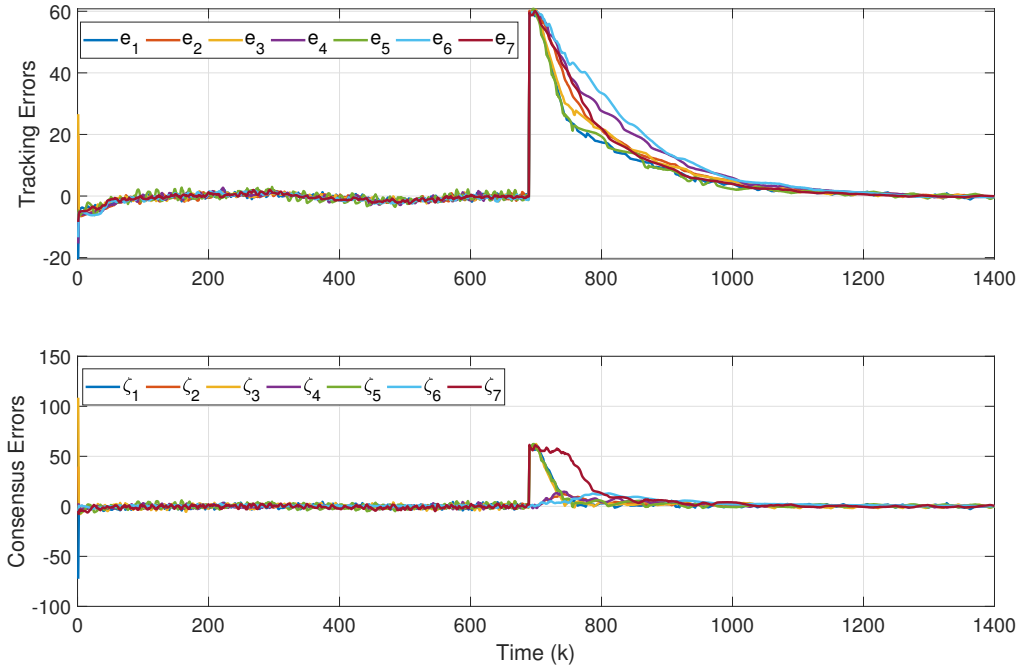

Figure 5. Tracking errors and Consensus errors of agent $\imath$.

6. Conclusions

This paper investigated the leader-following consensus problem for discrete-time nonlinear multi-agent systems under dynamic sparse attacks and disturbances. By integrating a dynamic linearization technique with 4a DDETM, a secure data-driven control framework was established, where a dynamic linearization technique first establishes an equivalent error model using only I/O data. To enhance security and save bandwidth, a distributed dynamic event-triggered mechanism limits data transmission, while a dual-key encryption scheme coupled with a data-fusion algorithm preserves privacy and ensures reliable estimation. The proposed FDMFASMC algorithm eliminates the need for accurate system models and global topology information, making it highly suitable for large-scale applications. Future work will focus on extending this framework to heterogeneous MASs with switching topologies.

Author Contributions

G.T.: conceptualization, methodology, software, data curation, writing—riginal draft preparation; X.L.: visualization, investigation, supervision, software, validation; X.J.: writing—reviewing and editing. All authors have read and agreed to the published version of the manuscript.

Funding

This work was funded by National Science and Technology Major Project (J2019-V-0010-0105).

Institutional Review Board Statement

Not applicable.

Informed Consent Statement

Not applicable.

Data Availability Statement

Not applicable.

Conflicts of Interest

The authors declare no conflict of interest.

Use of AI and AI-Assisted Technologies

No AI tools were utilized for this paper.

References

1. Xie, M.; Wu, Z.; Huang, H. Low-Complexity Formation Control of Marine Vehicle System Based on Prescribed Performance. *Nonlinear Dyn.* **2024**, *112*, 18311–18332.
2. Wang, L.; Zhu, D.; Pang, W.; et al. A Novel Obstacle Avoidance Consensus Control for Multi-AUV Formation System. *IEEE/CAA J. Autom. Sin.* **2023**, *10*, 1304–1318.
3. Zhang, D.; Feng, G.; Shi, Y.; et al. Physical Safety and Cyber Security Analysis of Multi-Agent Systems: A Survey of Recent Advances. *IEEE/CAA J. Autom. Sin.* **2021**, *8*, 319–333.
4. Dai, S.L.; He, S.; Cai, H.; et al. Adaptive Leader-Follower Formation Control of Underactuated Surface Vehicles with Guaranteed Performance. *IEEE Trans. Syst. Man Cybern. Syst.* **2022**, *52*, 1997–2008.
5. Ma, L.; Wang, Y.L.; Han, Q.L. Cooperative Target Tracking of Multiple Autonomous Surface Vehicles Under Switching Interaction Topologies. *IEEE/CAA J. Autom. Sin.* **2023**, *10*, 673–684.
6. Chen, G.; Zhou, Q.; Ren, H.; et al. Sensor-Fusion-Based Event-Triggered Following Control for Nonlinear Autonomous Vehicles Under Sensor Attacks. *IEEE Trans. Autom. Sci. Eng.* **2025**, *22*, 17411–17420.
7. Liu, J.; Fan, C.; Peng, Y.; et al. Emergent Leader-Follower Relationship in Networked Multi-Agent Systems. *Sci. China Inf. Sci.* **2023**, *66*, 229201.
8. Ren, Q.; Chen, G.; Peng, X.J.; et al. Secure Distributed Estimation-Based Data-Driven Leader-Following Control for Discrete-Time MASs Under Deception Attacks and Sensor Faults. *IEEE Trans. Netw. Sci. Eng.* **2026**, *13*, 1754–1769.
9. Zhai, S.; Wang, X.; Zheng, W.X. Leaderless Cluster Consensus of Second-Order General Nonlinear Multi-Agent Systems Under Directed Topology. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2023**, *70*, 4080–4091.
10. Wang, H.; Ren, W.; Yu, W.; et al. Fully Distributed Consensus Control for a Class of Disturbed Second-Order Multi-Agent Systems with Directed Networks. *Automatica* **2021**, *132*, 109816.

11. Li, N.; Zheng, W.X. Bipartite Synchronization of Multiple Memristor-Based Neural Networks with Antagonistic Interactions. *IEEE Trans. Neural Netw. Learn. Syst.* **2021**, *32*, 1642–1653.
12. Cai, Y.; Wang, Y.; Su, H.; et al. Bipartite Leader-Following Consensus of Linear Multi-Agent Systems with Unknown Disturbances Under Directed Graphs by Double Dynamic Event-Triggered Mechanism. *Appl. Math. Comput.* **2025**, *496*, 129347.
13. Hou, Z.; Jin, S. *Model Free Adaptive Control*; CRC Press: Boca Raton, FL, USA, 2013.
14. Bu, X.; Yu, Q.; Hou, Z.; et al. Model Free Adaptive Iterative Learning Consensus Tracking Control for a Class of Nonlinear Multi-Agent Systems. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 677–686.
15. Zhang, S.; Ma, L.; Yi, X. Model-Free Adaptive Control for Nonlinear Multi-Agent Systems with Encoding-Decoding Mechanism. *IEEE Trans. Signal Inf. Process. Netw.* **2022**, *8*, 489–498.
16. Hui, Y.; Chi, R.; Huang, B.; et al. Observer-Based Sampled-Data Model-Free Adaptive Control for Continuous-Time Nonlinear Nonaffine Systems with Input Rate Constraints. *IEEE Trans. Syst. Man Cybern. Syst.* **2021**, *51*, 7813–7822.
17. Bu, X.; Yu, W.; Yu, Q.; et al. Event-Triggered Model-Free Adaptive Iterative Learning Control for a Class of Nonlinear Systems Over Fading Channels. *IEEE Trans. Cybern.* **2022**, *52*, 9597–9608.
18. Yin, C.; Ren, H.; Li, H.; et al. Observer-Based Data-Driven Consensus Control for Nonlinear Multi-Agent Systems with Faded Neighborhood Information. *Inf. Sci.* **2023**, *649*, 119679.
19. Bao, Y.; Zhao, D.; Sun, J.; et al. Resilient Synchronization of Neural Networks Under DoS Attacks and Communication Delays via Event-Triggered Impulsive Control. *IEEE Trans. Syst. Man Cybern. Syst.* **2024**, *54*, 471–483.
20. Liu, G.; Park, J.H.; Hua, C.; et al. Dynamic Event-Triggered Consensus for Multi-Agent Systems Under DoS Attacks: A Hybrid System Approach. *IEEE Trans. Syst. Man Cybern. Syst.* **2023**, *53*, 7223–7233.
21. Zhao, W.; Lu, J.; Ren, F. Consensus of Heterogeneous Multi-Agent Networks Under Sparse Attacks by Integral-Type Observer. *IEEE Trans. Control Netw. Syst.* **2024**, *11*, 2064–2074.
22. Zhang, B.; Wang, D.; Wang, F. Data-Driven Distributed Model-Free Adaptive Predictive Control for Multiple High-Speed Trains Under False Data Injection Attacks. *Algorithms* **2025**, *18*, 267.
23. Deng, C.; Jin, X.Z.; Wu, Z.G.; et al. Data-Driven-Based Cooperative Resilient Learning Method for Nonlinear MASs Under DoS Attacks. *IEEE Trans. Neural Netw. Learn. Syst.* **2024**, *35*, 12107–12116.
24. Yu, W.; Wang, R.; Bu, X.; et al. Resilient Model-Free Adaptive Iterative Learning Control for Nonlinear Systems Under Periodic DoS Attacks via a Fading Channel. *IEEE Trans. Syst. Man Cybern. Syst.* **2022**, *52*, 4117–4128.
25. Duan, S.; Chen, G.; Zhou, Q.; et al. Fully Distributed Model-Free Adaptive Sliding Mode Control for MASs with Hybrid-Attacked Topology. *IEEE Trans. Autom. Sci. Eng.* **2025**, *22*, 12336–12346.
26. Chen, G.; Zhou, Q.; Li, H.; et al. Event-Triggered State Estimation and Control for Networked Nonlinear Systems Under Dynamic Sparse Attacks. *IEEE Trans. Netw. Sci. Eng.* **2024**, *11*, 1947–1958.
27. Bessa, I.; Trapiello, C.; Puig, V.; et al. Dual-Rate Control Framework with Safe Watermarking Against Deception Attacks. *IEEE Trans. Syst. Man Cybern. Syst.* **2022**, *52*, 7494–7506.
28. Zhang, K.; Li, Z.; Wang, Y.; et al. Privacy-Preserving Dynamic Average Consensus via State Decomposition: Case Study on Multi-Robot Formation Control. *Automatica* **2022**, *139*, 110182.
29. Liu, J.; Deng, Y.; Zha, L.; et al. Event-Based Privacy-Preserving Security Consensus of Multi-Agent Systems with Encryption-Decryption Mechanism. *Int. J. Robust Nonlinear Control* **2024**, *34*, 4787–4801.
30. Liu, D.; Yang, G.H. Prescribed Performance Model-Free Adaptive Integral Sliding Mode Control for Discrete-Time Nonlinear Systems. *IEEE Trans. Neural Netw. Learn. Syst.* **2019**, *30*, 2222–2230.
31. Wang, S.; Cao, Y.; Huang, T.; et al. Sliding Mode Control of Neural Networks via Continuous or Periodic Sampling Event-Triggering Algorithm. *Neural Netw.* **2020**, *121*, 140–147.
32. Guo, R.; Xu, S.; Guo, J. Sliding-Mode Synchronization Control of Complex-Valued Inertial Neural Networks with Leakage Delay and Time-Varying Delays. *IEEE Trans. Syst. Man Cybern. Syst.* **2023**, *53*, 1095–1103.
33. Zhang, Y.; Song, J. Nonlinear Leader-Following MASs Control: A Data-Driven Adaptive Sliding Mode Approach with Prescribed Performance. *Nonlinear Dyn.* **2022**, *108*, 349–361.
34. Xu, D.; Zhang, W.; Shi, P.; et al. Model-Free Cooperative Adaptive Sliding-Mode-Constrained Control for Multiple Linear Induction Traction Systems. *IEEE Trans. Cybern.* **2020**, *50*, 4076–4086.
35. Zhou, Q.; Yin, C.; Ma, H.; et al. Prescribed Performance Bipartite Consensus Control for MASs Under Data-Driven Strategy. *IEEE/CAA J. Autom. Sin.* **2025**, *12*, 937–946.
36. Ma, Y.S.; Che, W.W.; Deng, C. Event-Triggered Model-Free Adaptive Control for Nonlinear Cyber-Physical Systems with False Data Injection Attacks. *Int. J. Robust Nonlinear Control* **2022**, *32*, 2442–2452.
37. Shi, T.; Che, W.W. Dynamic Event-Triggered Data-Driven Iterative Learning Bipartite Tracking Control for Nonlinear MASs with Prescribed Performance. *Sci. China Inf. Sci.* **2025**, *68*, 112205.
38. Lin, N.; Peng, H.; Chi, R. Event-Triggered Data-Driven Iterative Learning Control for Multi-Agent Systems with FDI Attacks. *IEEE Internet Things J.* **2025**, *12*, 22036–22047.
39. Liang, J.; Bu, X.; Cui, L.; et al. Event-Triggered Asymmetric Bipartite Consensus Tracking for Nonlinear Multi-Agent Systems Based on Model-Free Adaptive Control. *IEEE/CAA J. Autom. Sin.* **2023**, *10*, 662–672.

40. Zhang, J.; Chai, S.C.; Zhang, B.H.; et al. Distributed Model-Free Sliding-Mode Predictive Control of Discrete-Time Second-Order Nonlinear Multiagent Systems with Delays. *IEEE Trans. Cybern.* **2022**, *52*, 12403–12413.
41. Chi, R.; Hui, Y.; Huang, B.; et al. Data-Driven Adaptive Consensus Learning from Network Topologies. *IEEE Trans. Neural Netw. Learn. Syst.* **2022**, *33*, 3487–3497.
42. Wang, S.; Liu, J.; Zha, L.; et al. Distributed Event-Triggered-Based Encrypted Control for Nonlinear Multi-Agent Systems via Privacy-Preserving Approach. *Nonlinear Dyn.* **2025**, *113*, 10127–10142.
43. Gao, C.; Wang, Z.; He, X.; et al. Fault-Tolerant Consensus Control for Multiagent Systems: An Encryption-Decryption Scheme. *IEEE Trans. Autom. Control* **2022**, *67*, 2560–2567.