Received: 20 September 2023 | Revised: 12 December 2023 | Accepted: 18 January 2024

DOI: 10.1002/rnc.7232

RESEARCH ARTICLE

WILEY

Event-based privacy-preserving security consensus of multi-agent systems with encryption–decryption mechanism

Jinliang Liu[1] | **Ying Deng**[2] | **Lijuan Zha**[3] | **Xiangpeng Xie**[4] | **Engang Tian**[5]

[1]School of Computer Science, Nanjing University of Information Science and Technology, Nanjing, China

[2]College of Information Engineering, Nanjing University of Finance and Economics, Nanjing, China

[3]School of Science, Nanjing Forestry University, Nanjing, China

[4]Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing, China

[5]School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai, China

Correspondence
Jinliang Liu, School of Computer Science, Nanjing University of Information Science and Technology, Nanjing, Jiangsu, China.
Email: liujinliang@vip.163.com

Funding information
National Natural Science Foundation of China, Grant/Award Numbers: 62373252, 62273174, 61973152; Natural Science Foundation of Jiangsu Province of China, Grant/Award Number: BK20211290

Abstract

The article concentrates on exploring the issue of privacy-preserving sliding mode consensus of multi-agent systems (MASs) with disturbance. An encryption and decryption algorithm has been proposed to address data security and privacy issues during data transmission. To optimize network resource allocation, a dynamic event-triggering mechanism has been introduced, which reduces the number of encrypted data while saving the computation cost. The consensus performance based on the sliding mode control strategy is achieved when the reachability of the slide-mode surface is guaranteed, and then the slide-mode controller is developed. Finally, an empirical demonstration through a numerical example validates the efficacy of the proposed strategy.

KEYWORDS

dynamic event-triggered mechanism (DETM), encryption–decryption algorithms, multi-agent systems, sliding mode control (SMC)

1 | INTRODUCTION

The study of multi-agent systems (MASs) has become increasingly important due to their prevalent use in diverse domains such as sensor networks,[1,2] robotic swarms,[3] and unmanned aerial vehicle systems.[4] In recent years, consensus control of MASs has attracted significant interest among scholars, playing a crucial role in achieving coordination and coherence among multiple agents.[5–8] For example, Li et al.[6] studied the consensus problem of MASs with sensor uncertainty. He et al.[9] conducted research on consistent control of linear MASs with actuator saturations. However, these achievements were all established in a secure network environment without considering the threat of eavesdropping attacks. As a result, this article investigates consensus control of MASs with encryption and decryption mechanisms to achieve privacy preservation. Additionally, interference and communication constraints pose substantial challenges to the design of consensus control strategies for MASs. Therefore, new approaches and strategies are required to address these challenges and ensure the consensus control of MASs in practical applications.

Sliding mode control (SMC), in contrast to static control strategies, possesses superior adaptability and robustness, which can effectively respond to complex environmental changes and uncertainties in the system.[10,11] Based on the principles of sliding mode theory, SMC leverages the dimension-reducing property of the sliding surface and the fast response capability of the sliding variable.[12] Unlike conventional control methods, SMC does not heavily rely on precise system models, showcasing its strong adaptability and fault tolerance.[13,14] Therefore, SMC has garnered significant attention in MASs and is widely applied to achieve consensus control. In Reference 15, an adaptive dynamic programming-based integral SMC approach is employed to achieve optimal consensus control of MASs. A new adaptive pseudo-PID SMC strategy has been proposed to address the fault-tolerant consensus problem with integral quadratic constraints and unknown actuator efficiency effects in Reference 16. Guo et al.[17] designed a novel fault-tolerant distributed sliding mode controller with fault compensation to address the consensus problem of MASs with actuator faults. Given the impressive performance of the SMC method and its advantages, it is reasonable to explore the consensus control of MASs via the SMC strategy.

In practical applications, the event-triggered strategy (ETS) has garnered widespread attention from researchers to address limited network bandwidth issues.[18,19] ETS allows information exchange only when certain events are triggered, which is advantageous to traditional time-triggered strategies.[20,21] By dynamically detecting and responding to events, ETS can improve overall system performance and reduce bandwidth consumption.[22,23] Various ETS have been designed and discussed in the literature, such as periodic event-triggered mechanism,[24] self-triggered mechanism,[25,26] and dynamic event-triggered mechanism (DETM). For achieving the quasi-consensus in MASs, Xie et al.[27] presented a novel hybrid event-triggered impulsive consensus protocol that enforces the occurrence of event pulses by employing proper triggering strategies. Chen et al.[28] proposed a DETM to solve the problem of containment formation control, which realizes dynamic adjustment of the triggering threshold by introducing an auxiliary variable for each agent. Nonetheless, the research on dynamic event-triggered consensus control of MASs is still limited while taking network security into consideration, which deserves further discussion.

Driven by the escalating complexity of systems and the mounting demand for security, network-related security has garnered increasing research interest.[29–31] In networked systems, security issues primarily stem from inherent vulnerabilities in network-based communication technologies, which render signal transmission via shared communication channels prone to network attacks and information breaches.[32–34] Given the significant reliance of MASs on network communication, it is of paramount importance to ensure the security and integrity of agent interactions in safeguarding sensitive data against unauthorized access and malicious attacks.[35–37] To maximize confidentiality and integrity during transmission, sensitive data can be transformed into an incomprehensible format through encryption algorithms. Only authorized recipients with the proper decryption keys can decode and restore the original data, effectively protecting it from unauthorized interception, tampering, or eavesdropping.[38–40] As a result, research on encryption and decryption algorithms for MASs has become a widely recognized research topic. In Reference 40, two fault-tolerant consistent control schemes based on encryption and decryption were proposed to ensure privacy-preserving. Pan et al.[41] employed a dynamic encryption and decryption scheme founded on sampled data to address privacy-preserving queuing control problems in vehicular network-physical systems. In light of these related findings, it is evident that the privacy-preserving secure SMC consensus problem of MASs based on encryption–decryption has rarely received attention.

Taking inspiration from the aforementioned discussions, this article proposes an event-triggered sliding mode consensus control method for MASs with disturbance. Firstly, a DETM is constructed for each agent to decide whether or not to transmit the sampled state of the agent. Then, an encryption algorithm is introduced to encrypt the triggered data for transmission. Similarly, a decryption algorithm is applied to decrypt the received ciphertext and recover the actual data. Moreover, a robust sliding mode control law is established, enabling agents to converge to a consensus state quickly even in the presence of disturbances. The key contributions of this study encompass the following aspects:

(1) An encryption and decryption algorithm is designed to address data security and privacy issues during transmission. In comparison with previous works,[42–44] the encryption and decryption algorithm in this article employs a dual-key encryption algorithm to enhance the level of data security while ensuring data accuracy.
(2) An innovative consensus control strategy based on a discrete SMC method is proposed. By designing appropriate event-trigger conditions and encryption–decryption mechanisms, the constructed SMC scheme can enable rapid convergence of all agents to a consensus state. Furthermore, sufficient conditions are provided to ensure both the security consensus of MASs and the reachability of the sliding surface. Finally, the accuracy of the encryption and decryption is verified through a simulation example.

Notations: $\mathbb{R}^m$ and $\mathbb{R}^{m\times n}$ represent the m-dimensional space and the set of $m\times n$ real matrices; $\otimes$ is the Kronecker product of two matrices; I represents the identity matrix of suitable dimension; To any symmetric matrix X, we define $\lambda_{\max}(X)$ as the maximum eigenvalue and $\lambda_{\min}(X)$ as the minimum eigenvalue. **sgn**(x) is symbolic function.

2 | PROBLEM FORMULATION

Figure 1 presents the block diagram of discrete MASs under DETM and encryption–decryption algorithms. After passing through the event generator, each agent generates the triggered state, which is then encrypted to generate ciphertext. The encrypted codewords are then transmitted to neighboring agents through the communication network. Upon receiving the codewords from neighboring agents, each agent employs a decryption algorithm to decrypt it and utilizes the decrypted value to update the control law.

2.1 | Graph theory

For a system comprising N agents, the data exchange among the agents constructs a connected graph $\mathcal{G}\triangleq\left(v,\varepsilon,\mathcal{A}_{\mathcal{G}}\right)$, where $v=\{v_1,v_2,\ldots,v_N\}$ denotes the set of nodes, and each node in the graph $\mathcal{G}$ represents an agent in MASs. The set of edges in the graph is denoted by $\varepsilon\subset v\times v$ and $\varepsilon_{ij}=\left(v_i,v_j\right)\in\varepsilon$ if there is an information flow from node v_i to node v_j, and $\mathcal{A}_{\mathcal{G}}=\left[a_{ij}\right]_{N\times N}$ is the adjacency matrix. The set of neighbors of node v_i is denoted by $\mathcal{N}_i=\left\{j|j\in v,j\neq i,\varepsilon_{ji}\in\varepsilon\right\}$ and the cardinality of $\mathcal{N}_i$ is denoted by d_i. $a_{ij}=1$ if and only if $\varepsilon_{ji}\in\varepsilon$, otherwise $a_{ij}=0$. In this article, we assume that the graph $\mathcal{G}$ is an undirected graph, hence $a_{ij}=a_{ji}$. The Laplacian matrix is denoted by $L=\left[l_{ij}\right]_{N\times N}$ with $l_{ii}=\sum_{j=1,j\neq i}^{N}a_{ij}$, $l_{ij}=-a_{ij}$, $i\neq j$.

2.2 | System description

In this article, the dynamics of MASs comprising N agents are expressed by the following:

$$x_i(k+1)=Ax_i(k)+B(u_i(k)+f_i(k)), \tag{1}$$

where $x_i(k)\in\mathbb{R}^n$, $u_i(k)\in\mathbb{R}^n$ and $f_i(k)$ represent the state variable, the input variable, and the actuator disturbance of agent i ($i\in 1,\ldots,N$).

Assumption 1. The nonlinear function $f_i(k)$ satisfies the condition:

$$\|f(k)\|\leq v\|x(k)\|, \tag{2}$$

where $v\geq 0$ is a known scalar.

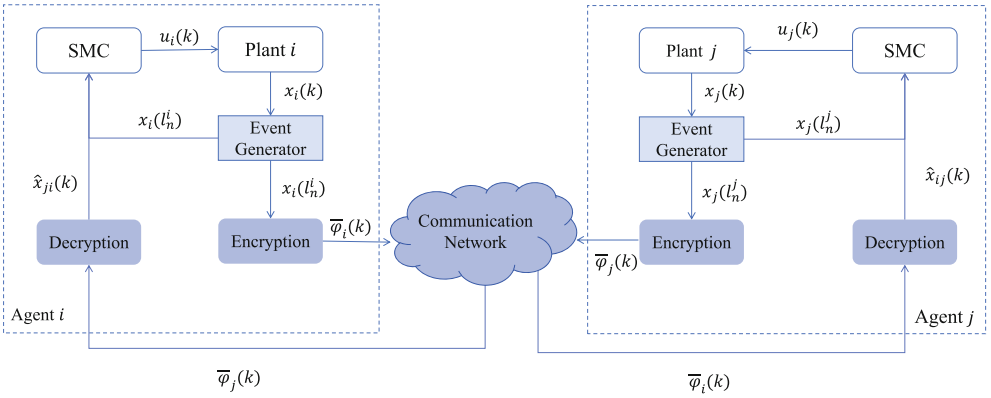

FIGURE 1 Communication structure diagram between agents.

2.3 | Design of DETM and encryption–decryption algorithm

In the considered MASs, the information exchange is via a shared open communication network which is constrained and vulnerable. To achieve the desired consensus performance, the issues of limited network bandwidth and information security should be well dealt with. In this article, the DETM is first utilized to alleviate the burden on communication resources. Then, to bolster the integrity and privacy of transmission data triggered by DETM, a proprietary encryption and decryption algorithm will be designed. The objective of these measures is to enhance the efficiency of communication resource utilization while ensuring secure data transmission and protecting agent privacy.

As shown in Figure 1, the transmitted state of agent i is determined by an event generator, and the triggering condition is set as

$$\frac{1}{\gamma}\phi_i(k) + \theta_1 x_i^{\mathrm{T}}(k)x_i(k) - \theta_2 q_i^{\mathrm{T}}(k)q_i(k) \leq 0, \tag{3}$$

where γ, θ_1, and θ_2 are given positive scalars, and $q_i(k) = x_i\left(l_n^i\right) - x_i(k)$, $x_i(l_n^i)$ denote the state of agent i at the l_n^i trigger time. Dynamic variable $\phi_i(k)$ satisfies

$$\phi_i(k+1) = \beta\phi_i(k) + \theta_1 x_i^{\mathrm{T}}(k)x_i(k) - \theta_2 q_i^{\mathrm{T}}(k)q_i(k), \tag{4}$$

where $\beta \in (0,1)$ is a known constant, $\phi_i(0) \geq 0$ is the initial condition.

The triggering sequence of agent i is described as $l_0^i, l_1^i, \ldots$. Thus, based on (3), the triggering sequence at agent i is denoted as:

$$l_{n+1}^i = \inf\left\{k > l_n^i | \textit{satisfying } (3)\right\}, \tag{5}$$

with $l_0^i = 0$.

Remark 1. Clearly, the DETM (6) is dependent on the parameters γ, θ_1 and θ_2. If $\gamma \to \infty$, the DETM (6) can be reduced to the static one. Notice that the threshold $\phi_i(k)$ can be dynamically adjusted based on the current state of the agent and the error $q_i(k)$. Under DETM (6), we can achieve a better balance between the system performance and the efficient use of network bandwidth by selecting appropriate parameters.

Considering the potential presence of eavesdroppers and information leakage in the communication network, an encryption–decryption algorithm will be introduced to ensure data security. As depicted in Figure 1, the transmitted state of agents will be encrypted by an encryptor before being conveyed over the network to the adjacent agent. Then the controller is proposed based on the decrypted data obtained from the received information. The encryption algorithm of agent i is described as

$$\begin{cases} \varphi_i(k) = \frac{x_i(l_n^i) - A\xi_i(k-1)}{g(k-1)} + g(k-1)\mathbf{1_N}, \\ \xi_i(k) = A\xi_i(k-1) + g(k-1)(\varphi_i(k) - g(k-1)\mathbf{1_N}), \\ \xi_i(0) = \mathbf{0}, \\ \overline{\varphi}_i(k) = M_k\varphi_i(k), \end{cases} \tag{6}$$

where the privacy matrix M_k is nonsingular. To obtain the codeword $\varphi_i(k)$ that should be transmitted to neighboring agents, an auxiliary variable $\xi_i(k)$ is introduced. It should be noted that $\varphi_i(k)$ cannot be decrypted without knowledge of the bounded scaling function $g(k)$, which can be considered as a symmetric key ensuring the confidentiality of the received information. $\overline{\varphi}_i(k)$ represents the encrypted data from agent i and transmitted into the network for communication.

Then, when agent i receives encrypted data $\overline{\varphi}_j(k)$, the decrypted data can be obtained using the key $g(k)$ and the privacy matrix M_k. The decryption algorithm of agent i is given by

$$\begin{cases} \varphi_j(k) = M_k^{-1}\overline{\varphi}_j(k), \\ \hat{x}_{ji}(k) = A\hat{x}_{ji}(k-1) + g(k-1)(\varphi_j(k) - g(k-1)\mathbf{1_N}), \\ \hat{x}_{ji}(0) = \mathbf{0}, \quad j \in \mathcal{N}_i, \end{cases} \tag{7}$$

where $\hat{x}_{ji}(k)$ is the state obtained after decryption.

Remark 2. According to the encryption and decryption algorithm described in this article, the encrypted value $\overline{\varphi}_j(k)$ of $x_j(l_n^j)$ is transmitted to agent i. By using algorithm (7), $\hat{x}_{ji}(k)$ can be obtained from $\overline{\varphi}_j(k)$. Based on equations (6) and (7), it can be easily derived that $\hat{x}_{ji}(k) = \xi_j(k) = x_j(l_n^j)$

Remark 3. It should be noted that the privacy matrix M_k in (6) and (7) can vary over time and also serve as a form of a key. M_k can be designed according to the specific requirements of the practical application scenarios, thereby adjusting the difficulty of the encryption and decryption algorithms. For example, in this article, M_k is designed as the product of $m(k)$ and $\overline{M}$, where the non-singular matrix $\overline{M}$ serves as a predefined seed, and the time-varying function $m(k) \neq 0$ generates time-varying coefficients.

2.4 | Design of SMC law

In this section, we will design an appropriate SMC strategy under DETM and an encryption–decryption scheme for achieving the consensus of the MASs. The sliding mode surface (SMS) function is selected as:

$$s_i(k) = Hz_i(k), \tag{8}$$

where H is a given parameter matrix. $z_i(k)$ is is an auxiliary variable defined as follows:

$$z_i(k) = \sum_{j=1}^{N} a_{ij}\big(x_i(k) - x_j(k)\big). \tag{9}$$

Considering DETM and encryption–decryption algorithm, (9) can be modified to:

$$\begin{aligned}\tilde{z}_i(k) &= \sum_{j=1}^{N} a_{ij}\big(x_i(l_n^i) - \hat{x}_{ji}(k)\big)\\ &= \sum_{j=1}^{N} a_{ij}(x_i(l_n^i) - x_i(k) + x_i(k) - x_j(k) + x_j(k) - x_j(l_n^j))\\ &= \sum_{j=1}^{N} a_{ij}\big(q_i(k) - q_j(k) + x_i(k) - x_j(k)\big).\end{aligned} \tag{10}$$

The sliding mode control law is designed in the following form:

$$u_i(k) = -K\tilde{z}_i(k) - \psi_i(k)\,\mathbf{sgn}\,(\tilde{s}_i(k)), \tag{11}$$

where $\tilde{s}_i(k) = H\tilde{z}_i(k)$, $\psi_i(k) = \overline{\psi}\|\tilde{z}_i(k)\|$, $\overline{\psi}$ is a given scalar, K represents control gains.

For the convenience of subsequent analysis, the following definitions are given:

$$z(k) \triangleq \mathrm{col}_N\{z_i(k)\},\ \tilde{z}(k) \triangleq \mathrm{col}_N\{\tilde{z}_i(k)\},\ q(k) \triangleq \mathrm{col}_N\{q_i(k)\},\ x(k) \triangleq \mathrm{col}_N\{x_i(k)\},$$

$$s(k) \triangleq \mathrm{col}_N\{s_i(k)\},\ u(k) \triangleq \mathrm{col}_N\{u_i(k)\},\ \tilde{s}(k) \triangleq \mathrm{col}_N\{\tilde{s}_i(k)\},\ \psi(k) \triangleq \mathrm{col}_N\{\psi_i(k)\}$$

Thus, the global forms of equations (8), (10), and (11) are as follows:

$$s(k) = (I_N \otimes H)z(k), \tag{12}$$

$$\tilde{z}(k) = (L \otimes I_n)(q(k) + x(k)), \tag{13}$$

$$u(k) = -(I_N \otimes K)\tilde{z}(k) - \psi(k)\mathbf{sgn}(\tilde{s}(k)). \tag{14}$$

Combining the definition of $x(k)$, (14) and (1), one can derive

$$\begin{aligned} x(k+1) &= (I_N \otimes A)x(k) + (I_N \otimes B)u(k) + (I_N \otimes B)f(k) \\ &= (I_N \otimes A - L \otimes BK)x(k) - (L \otimes BK)q(k) + (I_N \otimes B)F(k), \end{aligned} \tag{15}$$

where $F(k) = f(k) - \psi(k)\mathbf{sgn}(\tilde{s}(k))$.

Remark 4. The issue of sliding mode consensus control of MASs has been receiving significant attention in recent research. In Reference 13, a stochastic communication protocol-based SMC method was introduced to solve the consensus problem in MASs. In Reference 18, the event-triggered sliding mode tracking consensus control problem in MASs was investigated. In comparison with these works, this article is the first to consider the issue of sliding mode privacy-preserving control for MASs under DETM, and the proposed method has flexibility and security.

Definition 1 (40). The consensus of MASs is achieved if

$$\lim_{k\to\infty} \|x_i(k) - x_j(k)\| = 0, \quad i,j = 1,2,\ \dots\ ,N. \tag{16}$$

3 | MAIN RESULTS

In this section, a sufficient condition is firstly presented that ensures the stability of the system (15) under the DETM and encryption–decryption mechanism. Subsequently, the accessibility of the sliding mode surface (12) is discussed. Then, the gain of the consensus controller is designed based on sufficient conditions.

3.1 | Secure consensus analysis

To describe the consensus error, the concept of the average state will be defined

$$\bar{x}(k) = \frac{1}{N}\sum_{i=0}^{n} x_i(k). \tag{17}$$

Then, the consensus error can be obtained:

$$\begin{aligned} \tilde{x}(k+1) &= x(k+1) - \bar{x}(k+1) \\ &= (\tilde{N} \otimes I_n)x(k+1) \\ &= (\tilde{N} \otimes A)x(k) + (\tilde{N} \otimes B)u(k) + (\tilde{N} \otimes B)f(k) \\ &= (\tilde{N} \otimes A - \tilde{N}L \otimes BK)x(k) - (\tilde{N}L \otimes BK)q(k) + (\tilde{N} \otimes B)F(k). \end{aligned} \tag{18}$$

where $\tilde{N} = I_N - \frac{1}{N}\mathbf{1_N}\mathbf{1_N^T}$.

Next, based on (18), the main result regarding the consensus issue of MASs (1) will be discussed.

Theorem 1. *For the MASs (1), by considering the DETM (5) and the distributed sliding mode controller (12), if the defined DET parameters in (3)–(4) satisfy* $\beta\gamma \geq 1$, *and there exists a symmetric matrix* $P_1 > 0$ *and a scalar* $\omega_1 > 0$ *satisfying the following matrix inequalities*:

$$(\tilde{N} \otimes B)^{\mathrm{T}} P_1 (\tilde{N} \otimes B) \leq \omega_1 I, \tag{19}$$

$$\Pi = \begin{bmatrix} \Pi_{11} & * & * \\ \Pi_{21} & \Pi_{22} & * \\ 0 & 0 & \Pi_{33} \end{bmatrix} < 0, \tag{20}$$

where

$$\Pi_{11} = 2(\mathbb{A}-\mathbb{B})^{\mathrm{T}}P_1(\mathbb{A}-\mathbb{B}) + 4\omega_1 v^2 I + 8\omega_1\overline{\psi}^2\tilde{L}^{\mathrm{T}}\tilde{L} + \frac{\theta_1}{\gamma}I - (\tilde{N}\otimes I_n)^{\mathrm{T}}P_1(\tilde{N}\otimes I_n), \quad \Pi_{21} = -2(\mathbb{A}-\mathbb{B})^{\mathrm{T}}P_1\mathbb{B},$$

$$\Pi_{22} = 2\mathbb{B}^{\mathrm{T}}P_1\mathbb{B} + 8\omega_1\overline{\psi}^2\tilde{L}^{\mathrm{T}}\tilde{L} - \frac{\theta_2}{\gamma}I, \quad \Pi_{33} = -\frac{1-\beta}{\gamma}, \quad \mathbb{A} = \tilde{N}\otimes A, \quad \mathbb{B} = \tilde{N}L\otimes BK, \quad \tilde{L} = L\otimes I_n,$$

the consensus error system (18) is asymptotic stable.

Proof. From (3), one can easily get

$$\beta\phi(k) + \theta_1 x^{\mathrm{T}}(k)x(k) - \theta_2 q^{\mathrm{T}}(k)q(k) \geq 0.$$

According to the dynamical equation (4), it can be noticed that

$$\phi(k+1) \geq \left(\beta-\gamma^{-1}\right)\phi(k) \geq \cdots \geq \left(\beta-\gamma^{-1}\right)^{k+1}\phi(0).$$

It is evident that $\phi(k) \geq 0$.

Then, consider the Lyapunov function as

$$V_1(k) = \tilde{x}^{\mathrm{T}}(k)P_1\tilde{x}(k) + \frac{1}{\gamma}\phi(k). \tag{21}$$

From (2) and the definition of $F(k)$ in (15), the following inequality can be derived:

$$\|F(k)\| \leq v\|x(k)\| + \overline{\psi}\|\tilde{z}(k)\|. \tag{22}$$

Furthermore, according to (13), (18), (19), and (22), we can obtain

$$\begin{aligned}
&\tilde{x}^{\mathrm{T}}(k+1)P_1\tilde{x}(k+1)\\
&= \left[(\tilde{N}\otimes A - \tilde{N}L\otimes BK)x(k) - (\tilde{N}L\otimes BK)q(k) + (\tilde{N}\otimes B)F(k)\right]^{\mathrm{T}}P_1\left[(\tilde{N}\otimes A - \tilde{N}L\otimes BK)x(k)\right.\\
&\quad \left. - (\tilde{N}L\otimes BK)q(k) + (\tilde{N}\otimes B)F(k)\right]\\
&\leq 2[(\tilde{N}\otimes A - \tilde{N}L\otimes BK)x(k) - (\tilde{N}L\otimes BK)q(k)]^{\mathrm{T}}P_1\left[(\tilde{N}\otimes A - \tilde{N}L\otimes BK)x(k) - (\tilde{N}L\otimes_B K)q(k)\right]\\
&\quad + 2\omega_1 F^{\mathrm{T}}(k)F(k)\\
&\leq 2\left[(\tilde{N}\otimes A - \tilde{N}L\otimes BK)x(k) - (\tilde{N}L\otimes BK)q(k)\right]^{\mathrm{T}}P_1\left[(\tilde{N}\otimes A - \tilde{N}L\otimes BK)x(k) - (\tilde{N}L\otimes BK)q(k)\right]\\
&\quad + 4\omega_1 v^2 x^{\mathrm{T}}(k)x(k) + 4\omega_1\overline{\psi}^2\left[(q(k)+x(k))^{\mathrm{T}}(L\otimes I_n)^{\mathrm{T}}(L\otimes I_n)(q(k)+x(k))\right]\\
&\leq 2\left[(\mathbb{A}-\mathbb{B})x(k) - \mathbb{B}q(k)\right]^{\mathrm{T}}P_1\left[(\mathbb{A}-\mathbb{B})x(k) - \mathbb{B}q(k)\right] + 4\omega_1 v^2 x^{\mathrm{T}}(k)x(k)\\
&\quad + 8\omega_1\overline{\psi}^2\left[q(k)^{\mathrm{T}}\tilde{L}^{\mathrm{T}}\tilde{L}q(k) + x(k)^{\mathrm{T}}\tilde{L}^{\mathrm{T}}\tilde{L}x(k)\right].
\end{aligned} \tag{23}$$

Thus, the difference of the Lyapunov function (21) is

$$\begin{aligned}
\Delta V_1(k) &= \tilde{x}^{\mathrm{T}}(k+1)P_1\tilde{x}(k+1) + \frac{1}{\gamma}(\phi(k+1)-\phi(k)) - \tilde{x}^{\mathrm{T}}(k)P_1\tilde{x}(k)\\
&\leq 2\left[(\mathbb{A}-\mathbb{B})x(k) - \mathbb{B}q(k)\right]^{\mathrm{T}}P_1\left[(\mathbb{A}-\mathbb{B})x(k) - \mathbb{B}q(k)\right] + 4\omega_1 v^2 x^{\mathrm{T}}(k)x(k)\\
&\quad + 8\omega_1\overline{\psi}^2[q(k)^{\mathrm{T}}\tilde{L}^{\mathrm{T}}\tilde{L}q(k) + x(k)^{\mathrm{T}}\tilde{L}^{\mathrm{T}}\tilde{L}x(k)] + \frac{\theta_1}{\gamma}x^{\mathrm{T}}(k)x(k) - \frac{\theta_2}{\gamma}q^{\mathrm{T}}(k)q(k) + \frac{\beta-1}{\gamma}\phi(k)\\
&\quad - x^{\mathrm{T}}(k)(\tilde{N}\otimes I_n)^{\mathrm{T}}P_1(\tilde{N}\otimes I_n)x(k)\\
&\leq \eta^{\mathrm{T}}(k)\Pi\eta(k),
\end{aligned} \tag{24}$$

where $\eta(k) = [x^{\mathrm{T}}(k), q^{\mathrm{T}}(k), \sqrt{\phi(k)}]^{\mathrm{T}}$.

It is evident from (24) that the condition (20) ensures

$$\Delta V_1(k) \leq \eta^{\mathrm{T}}(k)\Pi\eta(k) < 0. \tag{25}$$

Therefore, the consensus error system is proved to be asymptotically stable, and the proof is concluded. ■

3.2 | Reachability analysis

Theorem 2 examines the accessibility of the designated sliding surface (8). The trajectory of MASs (8) can enter the sliding domain Θ.

Theorem 2. *Considering MASs (1) with the DETM and encryption–decryption mechanism, if there exists a symmetric matrix $P_2 > 0$, and a scalar $\omega_2 > 0$ satisfying the following matrix inequalities*:

$$(L \otimes HB)^{\mathrm{T}} P_2 (L \otimes HB) \leq \omega_2 I, \tag{26}$$

$$\vec{\Pi} = \begin{bmatrix} \vec{\Pi}_{11} & * & * \\ \vec{\Pi}_{21} & \vec{\Pi}_{22} & * \\ 0 & 0 & \Pi_{33} \end{bmatrix} < 0, \tag{27}$$

where

$$\vec{\Pi}_{11} = \Pi_{11} + 2(\tilde{A} - \tilde{B})^{\mathrm{T}} P_1 (\tilde{A} - \tilde{B}) + 4\omega_2 v^2 I, \vec{\Pi}_{21} = \Pi_{21} + 2(\tilde{A} - \tilde{B})^{\mathrm{T}} P_1 \tilde{B},$$
$$\vec{\Pi}_{22} = \Pi_{22} + 2\tilde{B}^{\mathrm{T}} P_1 \tilde{B}, \tilde{A} = L \otimes HA, \tilde{B} = L^2 \otimes HBK,$$

the state trajectories can be directed toward the subsequent sliding region Θ when influenced by the SMC law (14):

$$\Theta \triangleq \left\{ s(k) \middle| \|s(k)\| \leq \sqrt{\frac{4\omega_2}{\lambda_{\min}(P_2)}} \overline{\psi} \|\tilde{z}(k)\| \right\}. \tag{28}$$

Proof. Take the Lyapunov function as

$$V_2(k) \triangleq V_1(k) + s^{\mathrm{T}}(k) P_2 s(k). \tag{29}$$

From the sliding function (12), we can get

$$\begin{aligned} s(k+1) &= (I_N \otimes H) z(k+1) \\ &= (L \otimes H) x(k+1) \\ &= (\tilde{A} - \tilde{B}) x(k) - \tilde{B} q(k) + (L \otimes HB) F(k). \end{aligned} \tag{30}$$

In light of (22) and (26), the following can be deduced

$$\begin{aligned} & s^{\mathrm{T}}(k+1) P_2 s(k+1) \\ &= [(\tilde{A} - \tilde{B}) x(k) - \tilde{B} q(k) + (L \otimes HB) F(k)]^{\mathrm{T}} P_2 [(\tilde{A} - \tilde{B}) x(k) - \tilde{B} q(k) + (L \otimes HB) F(k)] \\ &\leq 2[(\tilde{A} - \tilde{B}) x(k) - \tilde{B} q(k)]^{\mathrm{T}} P_2 [(\tilde{A} - \tilde{B}) x(k) - \tilde{B} q(k)] + 2\omega_2 F^{\mathrm{T}}(k) F(k) \\ &\leq 2[(\tilde{A} - \tilde{B}) x(k) - \tilde{B} q(k)]^{\mathrm{T}} P_2 [(\tilde{A} - \tilde{B}) x(k) - \tilde{B} q(k)] + 4\omega_2 v^2 x^{\mathrm{T}}(k) x(k) + 4\omega_2 \overline{\psi}^2 \|\tilde{z}(k)\|^2. \end{aligned} \tag{31}$$

Thus, using (24) and (31), it yields

$$\Delta V_2(k) = \Delta V_1(k) + s^{\mathrm{T}}(k+1) P_2 s(k+1) - s^{\mathrm{T}}(k) P_2 s(k)$$

$$\begin{aligned}
&\leq \eta^{\mathrm{T}}(k)\Pi\eta(k) + 4\omega_2 v^2 x^{\mathrm{T}}(k)x(k) + 2[(\tilde{A}-\tilde{B})x(k) - \tilde{B}q(k)]^{\mathrm{T}}P_2[(\tilde{A}-\tilde{B})x(k) - \tilde{B}q(k)] \\
&\quad + 4\omega_2\overline{\psi}^2\|\tilde{z}(k)\|^2 - \lambda_{\min}(P_2)\|s(k)\|^2 \\
&\leq \eta^{\mathrm{T}}(k)\vec{\Pi}\eta(k) - [\lambda_{\min}(P_2)\|s(k)\|^2 - 4\omega_2\overline{\psi}^2\|\tilde{z}(k)\|^2]. \qquad (32)
\end{aligned}$$

If the system trajectory does not reach the sliding region Θ, then $\|s(k)\| \geq \sqrt{\frac{4\omega_2}{\lambda_{\min}(P_2)}}\overline{\psi}\|\tilde{z}(k)\|$. Otherwise, the condition (27) causes

$$\Delta V_2(k) \leq \eta^{\mathrm{T}}(k)\vec{\Pi}\eta(k) < 0, \qquad (33)$$

which indicates that the consensus state trajectory of MASs ultimately converges to the predetermined sliding region. The SMC reachability proof is finished. ∎

3.3 | Controller design

Based on the sufficient conditions for the SMS (8) reachability and consensus of MASs (1) under DETM obtained in Theorems 1 and 2, the following theorem is derived to obtain the desired controller gains.

Theorem 3. *Considering MASs (1) with the DETM and encryption–decryption mechanism, if there exist matrices $P_1 > 0, P_2 > 0, Y > 0, \overline{K}$, and scalars $\omega_i > 0 (i = 1, 2)$ satisfying the matrix inequalities*:

$$\begin{bmatrix} -\omega_1 I & * \\ \tilde{N}\otimes B & -\overline{P}_1 \end{bmatrix} < 0, \qquad (34)$$

$$\begin{bmatrix} -\omega_2 I & * \\ L\otimes HB & -\overline{P}_2 \end{bmatrix} < 0, \qquad (35)$$

$$\Sigma = \begin{bmatrix} \Sigma_{11} & * & * & * \\ \Sigma_{21} & \Sigma_{22} & * & * \\ \Sigma_{31} & 0 & \Sigma_{33} & * \\ \Sigma_{41} & 0 & 0 & \Sigma_{44} \end{bmatrix} < 0, \qquad (36)$$

where

$$\Sigma_{11} = \begin{bmatrix} \overline{P}_1 - \tilde{Y}^{\mathrm{T}}(\tilde{N}\otimes I_n)^{\mathrm{T}} - (\tilde{N}\otimes I_n)\tilde{Y} & * & * \\ 0 & \frac{\gamma}{\theta_2}I - \tilde{Y}^{\mathrm{T}} - \tilde{Y} & * \\ 0 & 0 & -\frac{1-\beta}{\gamma} \end{bmatrix}, \quad \Sigma_{21} = \begin{bmatrix} \vec{\mathbb{A}}_1 & \vec{\mathbb{B}}_1 & 0 \\ \vec{\mathbb{A}}_2 & \vec{\mathbb{B}}_2 & 0 \end{bmatrix},$$

$$\Sigma_{22} = \begin{bmatrix} -\overline{P}_1 & 0 \\ 0 & -\overline{P}_2 \end{bmatrix}, \quad \Sigma_{31} = \begin{bmatrix} \tilde{Y} & 0 & 0 \\ (L\otimes I_n)\tilde{Y} & 0 & 0 \end{bmatrix}, \quad \Sigma_{41} = \begin{bmatrix} \tilde{Y} & 0 & 0 \\ \tilde{Y} & 0 & 0 \\ (L\otimes I_n)\tilde{Y} & 0 & 0 \end{bmatrix}, \quad \tilde{Y} = I_N \otimes Y,$$

$$\vec{\mathbb{A}}_1 \triangleq \sqrt{2}(\tilde{N}\otimes AY - \tilde{N}L\otimes B\overline{K}), \vec{\mathbb{B}}_1 \triangleq \sqrt{2}(\tilde{N}L\otimes B\overline{K}), \quad \vec{\mathbb{A}}_2 \triangleq \sqrt{2}(L\otimes HAY - L^2\otimes HB\overline{K}),$$

$$\vec{\mathbb{B}}_2 \triangleq \sqrt{2}(L^2\otimes HB\overline{K}), \quad \Sigma_{33} = diag\left\{-\frac{1}{4\omega_1 v^2}I, -\frac{1}{8\omega_1\overline{\psi}^2}I\right\}, \quad \Sigma_{44} = diag\left\{-\frac{\gamma}{\theta_1}I, -\frac{1}{4\omega_2 v^2}I, -\frac{1}{8\omega_2\overline{\psi}^2}I\right\},$$

the security consensus of MASs and the reachability of the SMS can be guaranteed.

Furthermore, the desired controller gain can be denoted by

$$K = \overline{K}Y^{-1}. \tag{37}$$

Proof. Denote $\overline{P}_1 = P_1^{-1}, \overline{P}_2 = P_2^{-1}$. According to (37) and schur complement, (34) and (35) can be obtained from (19) and (26). Pre-multiplying and post-multiplying (27) by $diag\{\tilde{Y}, \tilde{Y}, I\}$ and its transpose, and using Schur complement, it can be derived

$$\begin{bmatrix} \overline{\Sigma}_{11} & * & * & * \\ \Sigma_{21} & \Sigma_{22} & * & * \\ \Sigma_{31} & 0 & \Sigma_{33} & * \\ \Sigma_{41} & 0 & 0 & \Sigma_{44} \end{bmatrix} < 0, \tag{38}$$

where

$$\overline{\Sigma}_{11} = \begin{bmatrix} -\tilde{Y}^{\mathrm{T}}(\tilde{N} \otimes I_n)^{\mathrm{T}} P_1 (\tilde{N} \otimes I_n)\tilde{Y} & * & * \\ 0 & -\tilde{Y}^{\mathrm{T}} \frac{\theta_2}{\gamma} \tilde{Y} & * \\ 0 & 0 & \frac{\beta - 1}{\gamma} \end{bmatrix}.$$

Based on the same method as Reference 19, we can get $-\tilde{Y}^{\mathrm{T}}(\tilde{N} \otimes I_n)^{\mathrm{T}} P_1 (\tilde{N} \otimes I_n)\tilde{Y} \leq \overline{P}_1 - \tilde{Y}^{\mathrm{T}}(\tilde{N} \otimes I_n)^{\mathrm{T}} - (\tilde{N} \otimes I_n)\tilde{Y}$, $-\tilde{Y}^{\mathrm{T}} \frac{\theta_2}{\gamma} \tilde{Y} \leq (\frac{\theta_2}{\gamma})^{-1} I - \tilde{Y}^{\mathrm{T}} - \tilde{Y}$, and then (36) can be exactly derived. Therefore, the proof of Theorem 3 is completed. ∎

4 | ILLUSTRATIVE EXAMPLES

In this section, the feasibility of the suggested algorithm is illustrated through a numerical example. Consider MASs (1) with parameters as follows

$$A = \begin{bmatrix} -0.2 & 0.4 \\ -0.1 & 0.3 \end{bmatrix}, \quad B = \begin{bmatrix} -0.03 \\ -0.02 \end{bmatrix}, \quad H = \begin{bmatrix} 0.5 & -0.1 \end{bmatrix}.$$

The communication topology network of MASs is displayed in Figure 2. The Laplace matrix of the graph is

$$L = \begin{bmatrix} 2 & -1 & -1 & 0 \\ -1 & 1 & 0 & 0 \\ -1 & 0 & 2 & -1 \\ 0 & 0 & -1 & 1 \end{bmatrix}.$$

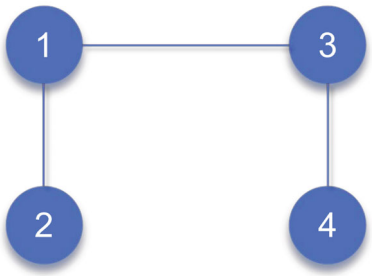

FIGURE 2 Communication graph.

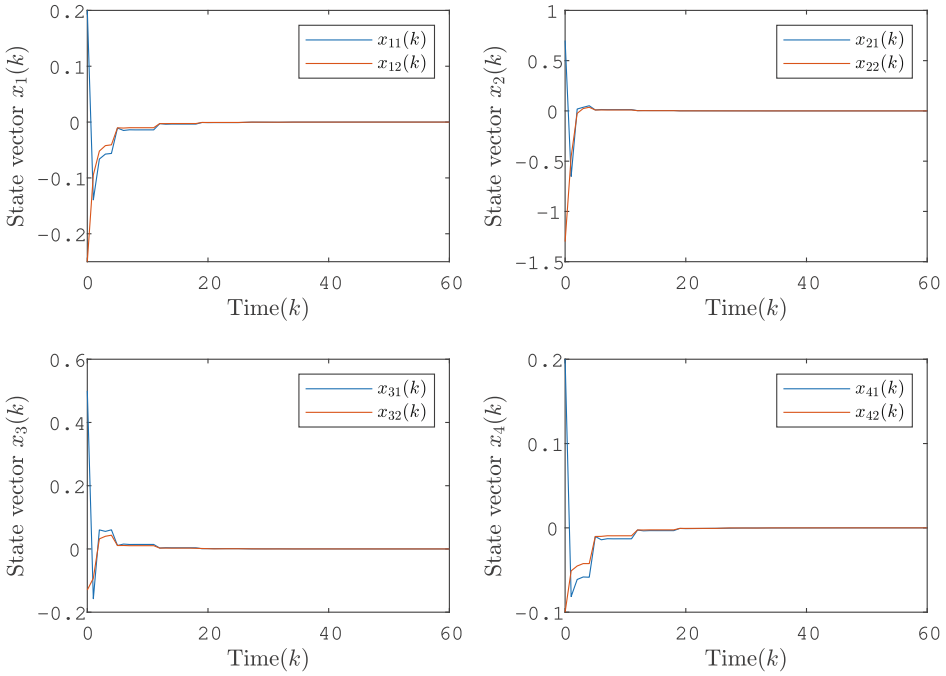

FIGURE 3 Responses of $x_i(k)$.

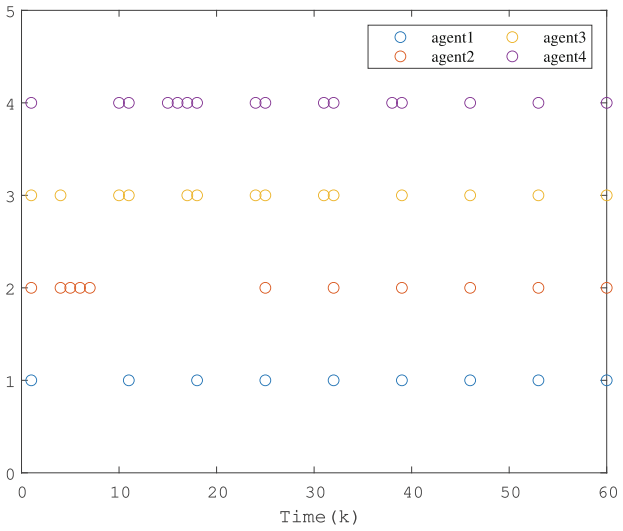

FIGURE 4 Event-triggered instants.

The matrix M_k in (6) is selected as:

$$m(k) = 2 + sin(-0.5k), \quad M_k = m(k) \times \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},$$

and the disturbance is $f_i(k) = 0.5sin(x_{i1}(k) + x_{i2}(k))$. The scaling function is chosen as $g(k) = 2 + sin(-0.8k)$. The initial state of the MASs are set as $x_1(0) = [0.2, -0.25]^{\mathrm{T}}, x_2(0) = [0.7, -1.3]^{\mathrm{T}}, x_3(0) = [0.5, -0.13]^{\mathrm{T}}, x_4(0) = [0.2, -0.1]^{\mathrm{T}}$. For given parameters $\gamma = 1.8, \beta = 0.6, \theta_1 = 78.1, \theta_2 = 12.7$, according to Theorem 3, the controller gain is obtained as $K = \begin{bmatrix} 0.1209 & 0.1039 \end{bmatrix}$.

Figures 3–8 display the simulation results of this article. The response of state $x(k)$, as shown in Figure 3, indicates that the state of agents achieves fast convergence under the DETM and encryption–decryption mechanism. Figure 4

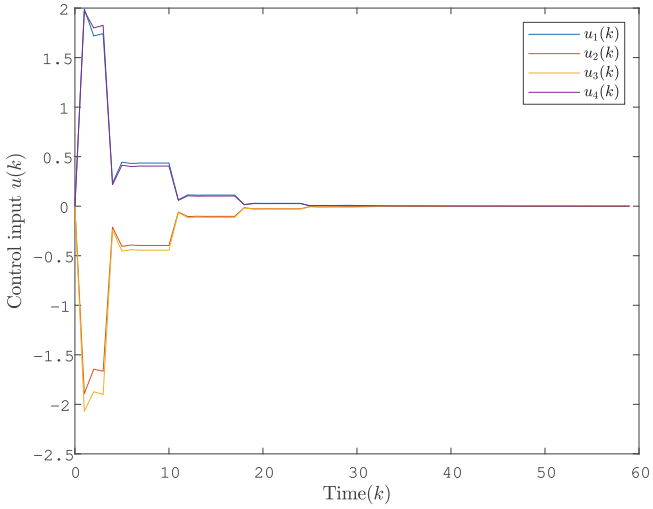

FIGURE 5 The control input $u_i(k)$.

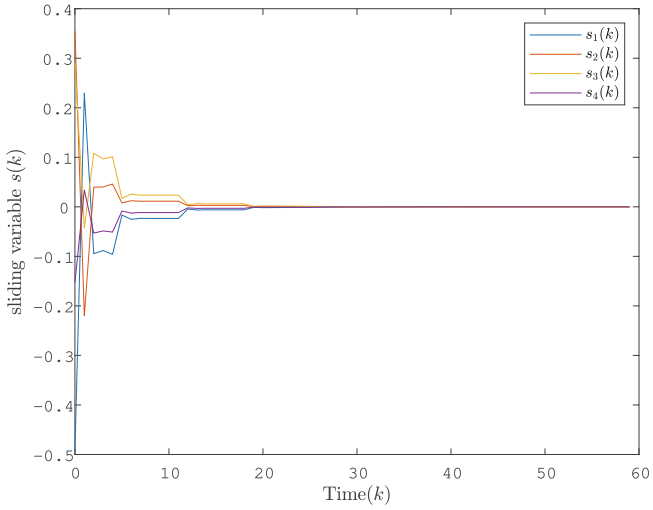

FIGURE 6 The sliding mode variables $s_i(k)$.

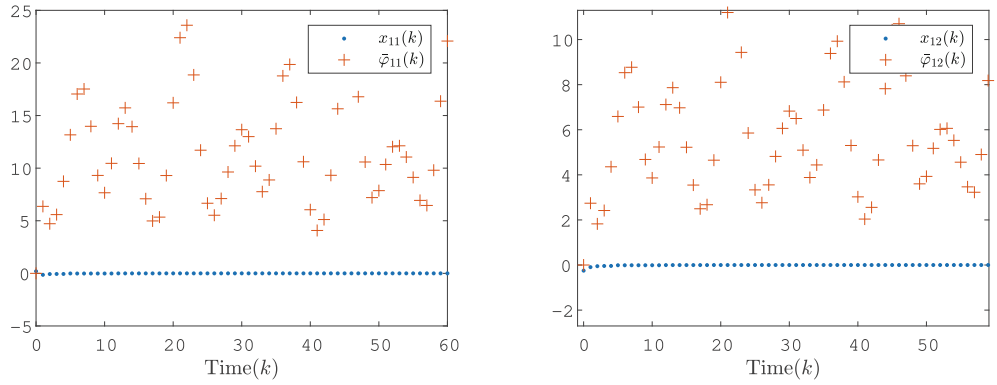

FIGURE 7 Encrypting $\overline{\varphi}_i(k)$ and state $x_i(l_n^i)$ for agent 1.

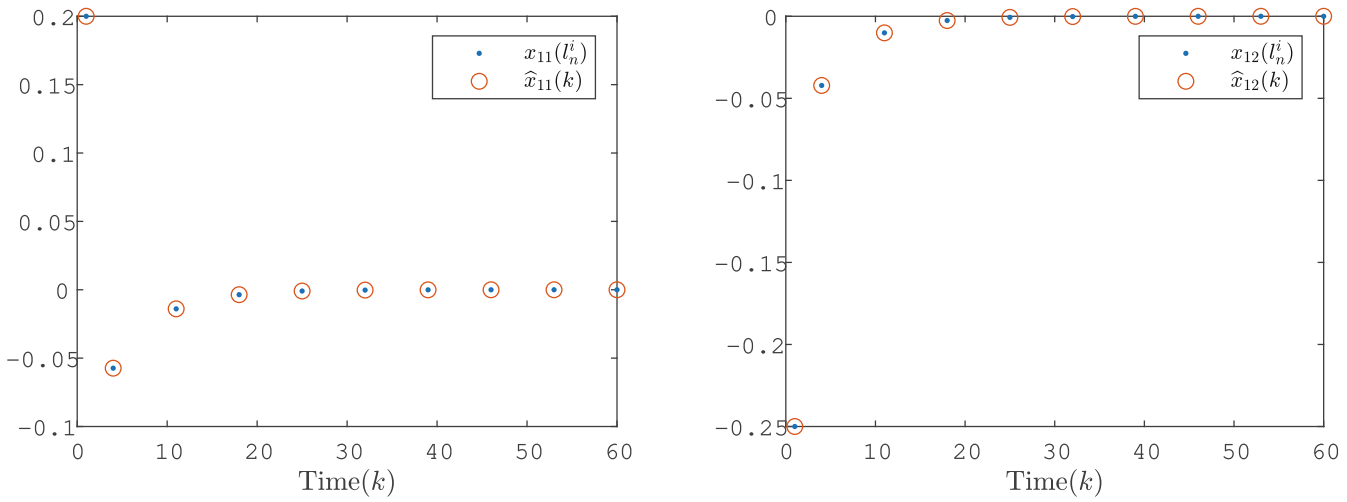

FIGURE 8 Decrypting $\hat{x}_{ij}(k)$ and state $x_i(l_n^i)$ for agent 1.

depicts the triggering instants and intervals of the four agents. The sliding variable $s(k)$ and the control inputs $u(k)$ for the SMC are given in Figures 5 and 6. Figure 7 presents the variations between the encrypted data transmitted over the network and the original data. The significant changes in Figure 7 indicate that this encryption–decryption mechanism has the capability to mitigate eavesdropping and information leakage issues in the network. Figure 8 demonstrates that the decrypted data precisely matches the original transferred data, confirming the encryption algorithm does not alter the values of the transmitted data. Based on the simulation results, it can be concluded that the proposed method in this article is able to achieve consensus of MASs while ensuring data confidentiality and integrity through encryption and decryption algorithms.

5 | CONCLUSION

This article investigates the privacy-preserving security consensus problem of perturbed MASs under DETM and SMC. To alleviate network bandwidth pressure, a DETM is employed to transmit data selectively. Moreover, an encryption and decryption algorithm is devised to safeguard the confidentiality and integrity of the transmitted information. Furthermore, a sliding mode controller is formulated based on the data signals received from adjacent agents, and sufficient conditions are established to guarantee consensus and reachability. Finally, the simulation results demonstrate the effectiveness of the proposed strategy. Future research directions may include privacy protection methods in multi-agent systems under more complex constraint conditions, especially in scenarios involving network attacks. These methods may involve different encryption and decryption techniques, as well as differential privacy methods that utilize noise for protection.

FUNDING INFORMATION
This work was supported by the National Natural Science Foundation of China (62373252, 62273174, 61973152), in part by the Natural Science Foundation of Jiangsu Province of China (BK20211290).

CONFLICT OF INTEREST STATEMENT
The authors declare no conflicts of interest.

DATA AVAILABILITY STATEMENT
Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

ORCID
Jinliang Liu https://orcid.org/0000-0001-5489-0246
Lijuan Zha https://orcid.org/0000-0003-0475-8866

Xiangpeng Xie https://orcid.org/0000-0003-4822-3134
Engang Tian https://orcid.org/0000-0002-8169-5347

REFERENCES

1. Li L, Shi P, Ahn CK. Distributed iterative FIR consensus filter for multiagent systems over sensor networks. *IEEE Trans Cybern*. 2022;52(6):4647-4660.
2. Kwon C, Hwang I. Sensing-based distributed state estimation for cooperative multiagent systems. *IEEE Trans Autom Control*. 2018;64(6):2368-2382.
3. Jin X, Dai SL, Liang J. Adaptive constrained formation-tracking control for a tractor-trailer mobile robot team with multiple constraints. *IEEE Trans Autom Control*. 2023;68(3):1700-1707.
4. Zou Y, Meng Z. Distributed hierarchical control for multiple vertical takeoff and landing UAVs with a distance-based network topology. *Int J Robust Nonlinear Control*. 2019;29(9):2573-2588.
5. Lu Y, Zhu M. Distributed economic control of dynamically coupled networks. *IEEE Trans Cybern*. 2020;52(3):1377-1391.
6. Li H, Xie L, Zhang X, Pan W. Distributed consensus control of nonlinear multi-agent systems with sensor uncertainty. *Int J Robust Nonlinear Control*. 2023;33(2):973-990.
7. Sarrafan N, Zarei J. Bounded observer-based consensus algorithm for robust finite-time tracking control of multiple nonholonomic chained-form systems. *IEEE Trans Autom Control*. 2021;66(10):4933-4938.
8. Wei L, Liao Y, Luo S, Chen WH, Huang G. Consensus of nonlinear multi-agent systems via distributed hybrid controls. *Int J Robust Nonlinear Control*. 2023;33(13):7510-7531.
9. He X, Wang Z, Gao C, Zhou D. Consensus control for multiagent systems under asymmetric actuator saturations with applications to mobile train lifting jack systems. *IEEE Trans Industr Inform*. 2023;19(10):10224-10232.
10. Song J, Wang Z, Niu Y, Hu J. Observer-based sliding mode control for state-saturated systems under weighted try-once-discard protocol. *Int J Robust Nonlinear Control*. 2020;30(18):7991-8006.
11. Yao D, Li H, Lu R, Shi Y. Distributed sliding-mode tracking control of second-order nonlinear multiagent systems: An event-triggered approach. *IEEE Trans Cybern*. 2020;50(9):3892-3902.
12. Zhang J, Lyu M, Shen T, Liu L, Bo Y. Sliding mode control for a class of nonlinear multi-agent system with time delay and uncertainties. *IEEE Trans Ind Electron*. 2017;65(1):865-875.
13. Li W, Niu Y, Cao Z, Lv X. Sliding mode control for multi-agent systems under stochastic communication protocol. *Int J Robust Nonlinear Control*. 2022;32(13):7522-7535.
14. Yang J, Li S, Yu X. Sliding-mode control for systems with mismatched uncertainties via a disturbance observer. *IEEE Trans Ind Electron*. 2012;60(1):160-169.
15. Zhang H, Park JH, Yue D, Zhao W. Nearly optimal integral sliding-mode consensus control for multiagent systems with disturbances. *IEEE Trans Syst Man Cybern Syst*. 2019;51(8):4741-4750.
16. Guo X, Tan D, Ahn CK, Wang JL. Fully distributed adaptive fault-tolerant sliding-mode control for nonlinear leader-following multiagent systems with ANASs and IQCs. *IEEE Trans Cybern*. 2020;52(5):2763-2774.
17. Guo X, Wei G, Ding D. Fault-tolerant consensus control for discrete-time multi-agent systems: A distributed adaptive sliding-mode scheme. *IEEE Trans Circuits Syst II Express Briefs*. 2023;70(7):2515-2519.
18. Nie R, He W, Du W, Lang Z, He S. Dynamic event-triggered SMC of multi-agent systems for consensus tracking. *IEEE Trans Circuits Syst II Express Briefs*. 2021;69(3):1188-1192.
19. Liu J, Gong E, Zha L, Tian E, Xie X. Interval type-2 fuzzy-model-based filtering for nonlinear systems with event-triggering weighted try-once-discard protocol and cyber-attacks. *IEEE Trans Fuzzy Syst*. 2023. doi:10.1109/TFUZZ.2023.3305088
20. Ding L, Han QL, Ge X, Zhang XM. An overview of recent advances in event-triggered consensus of multiagent systems. *IEEE Trans Cybern*. 2017;48(4):1110-1123.
21. Liu J, Zhang N, Zha L, Xie X, Tian E. Reinforcement learning-based decentralized control for networked interconnected systems with communication and control constraints. *IEEE Trans Autom Sci Eng*. 2023. doi:10.1109/TASE.2023.3300917
22. Ahmed I, Rehan M, Iqbal N. A novel exponential approach for dynamic event-triggered leaderless consensus of nonlinear multi-agent systems over directed graphs. *IEEE Trans Circuits Syst II Express Briefs*. 2021;69(3):1782-1786.
23. Wang S, Zheng S, Ahn CK, Shi P, Jiang X. Event-triggered cooperative control for uncertain multi-agent systems and applications. *Int J Robust Nonlinear Control*. 2023;33(12):7221-7245.
24. Heemels WPMH, Donkers MCF, Teel AR. Periodic event-triggered control for linear systems. *IEEE Trans Autom Control*. 2013;58(4):847-861.
25. Zhang H, Feng G, Yan H, Chen Q. Distributed self-triggered control for consensus of multi-agent systems. *IEEE/CAA J Automat Sinica*. 2014;1(1):40-45.
26. Zhang Y, Wu ZG, Shi P. Resilient event-/self-triggering leader-following consensus control of multiagent systems against DoS attacks. *IEEE Trans Industr Inform*. 2023;19(4):5925-5934.
27. Xie X, Wei T, Li X. Hybrid event-triggered approach for quasi-consensus of uncertain multi-agent systems with impulsive protocols. *IEEE Trans Circuits Syst I Reg Papers*. 2022;69(2):872-883.
28. Chen W, Wang Z, Ding D, Ghinea G, Liu H. Distributed formation-containment control for discrete-time multiagent systems under dynamic event-triggered transmission scheme. *IEEE Trans Syst Man Cybern Syst*. 2023;53(2):1308-1319.

29. Wang X, Tian E, Wei B, Liu J. Novel attack-defense framework for nonlinear complex networks: An important-data-based method. *Int J Robust Nonlinear Control*. 2023;33(4):2861-2878.
30. Tian E, Chen H, Wang C, Wang L. Security-ensured state of charge estimation of lithium-ion batteries subject to malicious attacks. *IEEE Trans Smart Grid*. 2023;14(3):2250-2261.
31. Zha L, Huang T, Liu J, Xie X, Tian E. Outlier-resistant quantized control for T-S fuzzy systems under multi-channel-enabled round-robin protocol and deception attacks. *Int J Robust Nonlinear Control*. 2023;33(18):10916-10931.
32. Wang Z, Wang L, Liu S, Wei G. Encoding-decoding-based control and filtering of networked systems: Insights, developments and opportunities. *IEEE/CAA J Automat Sinica*. 2018;5(1):3-18.
33. Liu J, Gong E, Zha L, Xie X, Tian E. Outlier-resistant recursive security filtering for multirate networked systems under fading measurements and round-Robin protocol. *IEEE Trans Control Netw Syst*. 2023;10(4):1962-1974. doi:10.1109/TCNS.2023.3256299
34. Peng C, Sun H. Switching-like event-triggered control for networked control systems under malicious denial of service attacks. *IEEE Trans Autom Control*. 2020;65(9):3943-3949.
35. Wang Y, Lu J, Zheng WX, Shi K. Privacy-preserving consensus for multi-agent systems via node decomposition strategy. *IEEE Trans Circuits Syst I Reg Papers*. 2021;68(8):3474-3484.
36. Liu L, Ma L, Guo J, Zhang J, Bo Y. Distributed set-membership filtering for time-varying systems: A coding–decoding-based approach. *Automatica*. 2021;129:109684.
37. Liang C, Ge M, Xu J, Liu Z, Liu F. Secure and privacy-preserving formation control for networked marine surface vehicles with sampled-data interactions. *IEEE Trans Veh Technol*. 2021;71(2):1307-1318.
38. Gao C, Wang Z, He X, Dong H. Encryption-decryption-based consensus control for multi-agent systems: Handling actuator faults. *Automatica*. 2021;134:109908.
39. Guo X, Wang B, Wang J, Ahn CK, Wu Z. Edge-event-triggered encryption-decryption observer-based control of multiagent systems for privacy protection under multiple cyber attacks. *Inf Sci*. 2023;642:119128.
40. Gao C, Wang Z, He X, Dong H. Fault-tolerant consensus control for multiagent systems: An encryption-decryption scheme. *IEEE Trans Autom Control*. 2021;67(5):2560-2567.
41. Pan D, Ding D, Ge X, Han QL, Zhang XM. Privacy-preserving platooning control of vehicular cyber-physical systems with saturated inputs. *IEEE Trans Syst Man Cybern Syst*. 2023;53(4):2083-2097.
42. Feng Y, Wang F, Duan F, Liu Z, Chen Z. Anonymous privacy-preserving consensus via mixed encryption communication. *IEEE Trans Circuits Syst II Express Briefs*. 2022;69(8):3445-3449.
43. Wang Z, Ma M, Zhou Q, et al. A privacy-preserving distributed control strategy in islanded AC Microgrids. *IEEE Trans Smart Grid*. 2022;13(5):3369-3382.
44. Gao L, Deng S, Ren W. Differentially private consensus with an event-triggered mechanism. *IEEE Trans Control Netw Syst*. 2019;6(1):60-71.

How to cite this article: Liu J, Deng Y, Zha L, Xie X, Tian E. Event-based privacy-preserving security consensus of multi-agent systems with encryption–decryption mechanism. *Int J Robust Nonlinear Control*. 2024;34(7):4787-4801. doi: 10.1002/rnc.7232