Frontiers of Information Technology & Electronic Engineering
www.jzus.zju.edu.cn engineering.cae.cn www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

Privacy-preserving bipartite consensus with cooperative–competitive interactions via a node decomposition strategy*

Licheng WANG[1], Yongling CHEN[2], Shuai LIU[‡2]

[1]*College of Automation Engineering, Shanghai University of Electric Power, Shanghai 200090, China*

[2]*College of Science, University of Shanghai for Science and Technology, Shanghai 200093, China*

E-mail: wanglicheng1217@163.com; chenyongling2024@163.com; liushuai871030@163.com

Received Feb. 14, 2025; Revision accepted July 31, 2025; Crosschecked Sept. 1, 2025; Published online Nov. 26, 2025

Abstract: This paper describes our investigation of the privacy protection problem of multi-agent systems under cooperative–competitive networks. A node decomposition strategy is used to protect the privacy of the initial node values, in which a node v_i is split into n_i nodes. By designing inter-node weights, the initial value of each node is protected from honest-but-curious nodes and eavesdroppers without relying on external algorithms. The purpose is to design a privacy-preserving consensus algorithm such that the privacy performance is guaranteed by using the node decomposition strategy, while the bipartite consensus is achieved for the cooperative–competitive multi-agent systems. Two numerical simulations are given to validate the effectiveness of the proposed privacy-preserving bipartite consensus algorithm.

Key words: Privacy-preserving; Bipartite consensus; Cooperative–competitive interactions; Multi-agent systems; Node decomposition

https://doi.org/10.1631/FITEE.2500093 **CLC number:** TP391.4

1 Introduction

With the development of control theory and its continuous integration with other disciplines, multi-agent systems based on the natural laws of group behaviors have proven to be a powerful tool to complete complex tasks (Mi et al., 2023; Li CY et al., 2024). Accordingly, the coordination control problem of multi-agent systems has attracted widespread attention in various fields (Yang et al., 2008; Wang LC et al., 2022; Huang, 2024; Zheng et al., 2024) due primarily to its low network resource consumption, fast execution speed, strong fault tolerance, and high reliability for tasks with a poor structural performance (Chanfreut et al., 2022; Wang LC et al., 2023, 2024, 2025; Fang et al., 2024). As the basis for cooperation and coordination in multi-agent systems, the consensus problem has been increasingly studied and achievements have been obtained (Talebi et al., 2006; Jiang et al., 2024).

In recent years, the consensus problem of multi-agent systems has been extended to various situations, such as second-order multi-agent systems (Wu XH and Mu, 2022), delayed multi-agent systems (Olfati-Saber and Murray, 2004), and cooperative–competitive networks (Dou and Song, 2023). In the study of multi-agent systems, a purely collaborative relationship between agents is often assumed, thus neglecting adversarial situations with negative connection weights (Zhai and Zheng, 2019). However, competitive relationships are indeed very common in multi-agent systems. For example, in robot soccer competitions, robots from different teams need

‡ Corresponding author

* Project supported by the National Natural Science Foundation of China (Nos. 62473247 and 62473261) and the Natural Science Foundation of Shanghai, China (Nos. 24ZR1425900 and 24ZR1453800)

ORCID: Shuai LIU, https://orcid.org/0000-0003-0523-022X

to compete to kick the ball into the opponent's goal. In distributed systems, different nodes may compete for limited computational resources or storage space. Altafini (2013) proved that the bipartite consensus problem in a structurally balanced signed network is equivalent to the standard consensus problem in a non-negative network under gauge transformation. To this end, some properties of standard consensus in non-negative networks can also apply to networks with cooperative–competitive relationships.

In networked systems (Yaghoubi et al., 2023; Liang et al., 2024), communication security challenges have become increasingly prominent (Sun LC et al., 2023; Sakthivel et al., 2024). Transmission channels are vulnerable to security threats such as eavesdropping and tampering. Against this backdrop, research on privacy-enhancing technologies has emerged as a critical area of focus. Up to now, homomorphic encryption and differential privacy have been the two most widely used methods to protect sensitive information (Kefayati et al., 2007; Li QX et al., 2019, 2020; Chen XM et al., 2023; Cheng et al., 2024; Wang W et al., 2024). Homomorphic encryption is a special encryption method that allows certain types of calculations to be performed directly on encrypted data without decryption (Gao H et al., 2018; Chen W et al., 2023; Gao PX et al., 2024). After computation, the result remains encrypted, and only those with the decryption key can view the computation result. This encryption method is very useful for protecting data privacy and achieving secure computation. Another widely used method is differential privacy. Differential privacy is a technique used to protect individual privacy, especially during data analysis and the release of statistical information. Because differential privacy is based on probability, all differential privacy methods must incorporate randomness (Mo and Murray, 2017; Wu L et al., 2023). Differential privacy mechanisms effectively ensure the privacy of the initial state values, but a major drawback is that they can only achieve average consensus in the probability sense (Zhang et al., 2023). To this end, it is necessary to balance the performance between the control accuracy and the privacy for differential privacy mechanisms.

Very recently, privacy protection methods based on state decomposition have been proposed by Wang YQ (2019) for undirected networks. The basic idea of this method is for each node to decompose its state into two sub-states with random initial values. Based on the aforementioned two-point decomposition mechanism, Wang YQ et al. (2021) proposed a new state decomposition method using a homomorphic encryption algorithm in undirected networks. This method decomposes each node into some sub-nodes. The number of these sub-nodes is based on the number of adjacent nodes, and they are interconnected in the form of a chain graph. Existing research has employed various specialized techniques to address the average consensus in privacy protection (Sun L et al., 2024), but only a few studies consider cooperative–competitive multi-agent systems. For example, Ma and Hu (2022) and Wang JM et al. (2024) investigated a safe consensus problem for cooperative–competitive multi-agent systems using a differential privacy approach. It should be pointed out that for cooperative–competitive multi-agent systems, there are the following challenges: (1) how to deal with the antagonistic topology structures; (2) how to quantify the information leakage level (Hoseinpour et al., 2024; Liu et al., 2024; Yuan et al., 2024).

Based on the above discussions, we aim to study the bipartite consensus problem of privacy protection in multi-agent systems with cooperation–competition networks using node decomposition which could accurately achieve privacy preservation. The main contributions of this paper are as follows:

1. The problem we address is new in the sense that several attempts are described to cope with the privacy protection bipartite consensus issue for cooperative competition multi-agent systems.

2. The node decomposition algorithm developed is new and covers the decomposition mechanism and the weight mechanism, based on which the privacy is protected while the bipartite consensus is achieved.

Notations The notations used in the paper are fairly standard except otherwise stated. $\mathbb{R}^n$ stands for the n-dimensional Euclidean space. $\boldsymbol{M}^{\mathrm{T}}$ represents the transpose of matrix $\boldsymbol{M}$. $\mathbf{1}$ denotes a column vector whose elements are all 1. The shorthand diag{} denotes a diagonal matrix. $\mathrm{sgn}(a)$ denotes a sign function; that is, if $a > 0$, $\mathrm{sgn}(a) = 1$, if $a = 0$, $\mathrm{sgn}(a) = 0$, and if $a < 0$, $\mathrm{sgn}(a) = -1$. $\mathrm{sp}(\boldsymbol{A}) = \mathrm{sp}(\boldsymbol{B})$ means that matrix $\boldsymbol{A}$ and matrix $\boldsymbol{B}$ are isospectral; that is, $\boldsymbol{A}$ and $\boldsymbol{B}$ have the same set of eigenvalues.

2 Preparatory knowledge and models

2.1 Graph theory

We consider an interactive topological network with n nodes. $\mathcal{G} = \{\mathcal{V}, \mathcal{E}, \boldsymbol{A}\}$ represents a signed graph, in which $\mathcal{V} = \{v_1, v_2, \ldots, v_n\}$ is the set of nodes, $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ is the set of edges, and $\boldsymbol{A} = [a_{i,j}]_{n\times n}$ is the adjacency matrix of the signed weights of $\mathcal{G}$. If $(v_j, v_i) \in \mathcal{E}$, the element $a_{i,j} = a_{ji} \neq 0$, and $a_{i,j} = 0$ otherwise. If $a_{i,j} > 0$, the weight between nodes v_i and v_j is positive, indicating a cooperative relationship between nodes v_i and v_j. If $a_{i,j} < 0$, the weight between nodes v_i and v_j is negative, indicating a competitive relationship between nodes v_i and v_j. $\boldsymbol{D}$ represents the degree matrix. $N_i = \{v_j \mid v_j \in \mathcal{V}, (v_i, v_j) \in \mathcal{E}\}$ is a set of neighbors of node v_i. There is $|N_i| = n_i$. N denotes the total number of edges.

2.2 Problem formulation

Consider a cooperative–competitive multi-agent system with n discrete-time agents as follows:

$$\boldsymbol{x}_i[k+1] = \boldsymbol{x}_i[k] + \varepsilon \boldsymbol{u}_i[k], \tag{1}$$

with the bipartite consensus protocol

$$\boldsymbol{u}_i[k] = -\sum_{v_j \in N_i} |a_{i,j}|(\boldsymbol{x}_i[k] - \mathrm{sgn}(a_{i,j})\boldsymbol{x}_j[k]), \tag{2}$$

where $\boldsymbol{x}_i \in \mathbb{R}^{n_x}$ is the state vector with n_x being the dimension of $\boldsymbol{x}_i$, $\boldsymbol{u}_i \in \mathbb{R}^{n_x}$ is the control input of agent i, and $\varepsilon \in (0, \frac{1}{\Delta})$ is a positive scalar with $\Delta \triangleq \max\limits_{i=1,2\ldots,n} |N_i|$.

The compact form of Eq. (1) can be written as

$$\boldsymbol{x}[k+1] = \boldsymbol{x}[k] - \varepsilon(\boldsymbol{D} - \boldsymbol{A})\boldsymbol{x}[k], \tag{3}$$

where $\boldsymbol{x}[k] \triangleq \mathrm{col}\{x_1[k], x_2[k], \ldots, x_n[k]\}$.

Applying the decomposition mechanism of Algorithm 1, the topology shown in Fig. 1 can be decomposed into the structure shown in Fig. 2. The black edge signifies a positive weight, the red edge denotes a negative weight, and the blue edge links nodes that originate from the same source. In this paper, the color of edges in other figures is the same as those in Figs. 1 and 2. Consequently, nodes joined by black and red edges are non-homologous, whereas nodes linked by the blue edge are considered homologous sub-nodes.

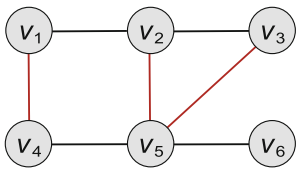

Fig. 1 Before node decomposition. References to color refer to the online version of this figure

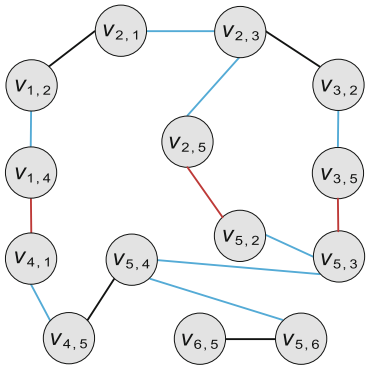

Fig. 2 After node decomposition. References to color refer to the online version of this figure

In traditional bipartite consensus algorithms, the initial values of nodes can be calculated by honest-but-curious nodes and eavesdroppers, which can lead to leakage of agent privacy. To protect the initial node values, this paper proposes a privacy-preserving scheme for cooperative–competitive multi-agent systems (1), which is based on a node decomposition strategy. The proposed privacy-preserving mechanism is divided into a decomposition mechanism and a weight mechanism. Next, we propose two algorithms to illustrate the specific decomposition mechanism (Algorithm 1) and the weight mechanism (Algorithm 2).

Through this privacy-preserving mechanism, system (1) can be decomposed into the following form:

$$\begin{aligned} &x_{i,j}[k+1] \\ =&x_{i,j}[k] + \varepsilon \sum_{v_j \in N_i} |a_{i,j}|(\mathrm{sgn}(a_{i,j})x_{j,i}[k] - x_{i,j}[k]) \\ &+ \varepsilon \sum_{\substack{v_p \in N_i, \\ v_{i,p} \in N(v_{i,j})}} a_i^{p,j}(x_{i,p}[k] - x_{i,j}[k]). \end{aligned} \tag{4}$$

It can be observed from Algorithm 1 that the privacy-preserving mechanism depends on the value range of $\underline{a}$ and $\bar{a}$ satisfying $0 < \underline{a} < \bar{a} < \frac{1}{\sqrt{\varepsilon\Delta}}$. After the node decomposition proposed in Algorithm 1,

the maximum number of neighbors of node v_i is 3, and $\frac{1}{\sqrt{\varepsilon\Delta}}$ is changed to $\frac{1}{\sqrt{3\varepsilon}}$. Therefore, one has $a_{i,j}=a_{j,i}\in(-\frac{1}{\sqrt{3\varepsilon}},\frac{1}{\sqrt{3\varepsilon}})$ and $a_i^{p,j}=a_i^{j,p}\in(0,\frac{1}{3\varepsilon})$.

Remark 1 It is worth noting that the decomposition strategy used in this study is the same as the node decomposition method according to Wang YQ et al. (2021), but with different weight mechanisms. According to Wang YQ et al. (2021), the transmission of information between nodes uses homomorphic encryption to prevent privacy leakage. However, this study does not involve homomorphic encryption algorithms, and instead, the privacy protection is achieved by directly designing weights. In this way, computational complexity is reduced.

Algorithm 1 Decomposition mechanism

Step 1: for any node v_i with $|N_i|=n_i$, the neighboring nodes of node v_i are sequentially represented as $v_1,v_2,\ldots,v_{n_i}$ and $1<2<\ldots<n_i$. Now we decompose node v_i into n_i sub-nodes, represented as $v_{i,1},v_{i,2},\ldots,v_{i,n_i}$ and those n_i sub-nodes are called homologous nodes. Then, we can totally get $2N$ sub-nodes.

Step 2: according to the subscripts of the decomposed sub-nodes $1,2,\ldots,n_i$, connect those sub-nodes in ascending order to obtain a chain graph, where those n_i sub-nodes are sequentially connected.

Step 3: perform the above two steps for each node in sequence.

Step 4: connect $v_{i,j}$ and $v_{j,i}$ where node $v_{i,j}$ is decomposed by node v_i and node $v_{j,i}$ is decomposed by node v_j. $v_{i,j}$ and $v_{j,i}$ are non-homologous sub-nodes. So, we can connect all the nodes with their neighbor nodes.

Step 5: define the sum of homologous child nodes that form one node as $\frac{2N}{n}$ of the original node, that is, $\sum_{q\in N_i}x_{i,q}[0]=\frac{2N}{n}x_i[0]$.

Algorithm 2 Weight mechanism

Step 1: after node decomposition, the weight between non-homologous child nodes $v_{i,j}$ remains consistent with the weight $a_{i,j}$ between nodes v_i and v_j before node decomposition, represented by $a_{i,j}$. Because the graph studied here is undirected, $a_{i,j}=a_{j,i}\in(-\frac{1}{\sqrt{3\varepsilon}},\frac{1}{\sqrt{3\varepsilon}})$.

Step 2: the weight between the homologous sub-nodes $v_{i,s}$ and $v_{i,r}$ is represented as $a_i^{r,s}$. The specific value of $a_i^{r,s}$ is designed in Section 4. In particular, the graph $\mathcal{G}$ is undirected, $a_i^{s,r}=a_i^{r,s}\in(0,\frac{1}{3\varepsilon})$.

Definition 1 An undirected signed graph is said to be structurally balanced if it admits a bipartition of the node sets $\mathcal{V}_1$ and $\mathcal{V}_2$, $\mathcal{V}_1\cap\mathcal{V}_2=\varnothing,\mathcal{V}_1\cup\mathcal{V}_2=\mathcal{V}$, such that $a_{i,j}\geq 0$, $\forall v_i,v_j\in\mathcal{V}_q$ $(q\in\{1,2\})$, $a_{i,j}\leq 0$, $v_i\in\mathcal{V}_p$, and $v_j\in\mathcal{V}_q$ $(p,q\in\{1,2\})$, $p\neq q$. It is said to be structurally unbalanced otherwise (Altafini, 2013).

Figs. 3 and 4 represent structurally balanced and structurally unbalanced graphs, respectively. Each negative edge is associated with a pair of nodes, one from set $\mathcal{V}_1$ and the other from set $\mathcal{V}_2$. Each positive edge links two nodes from either set $\mathcal{V}_1$ or set $\mathcal{V}_2$.

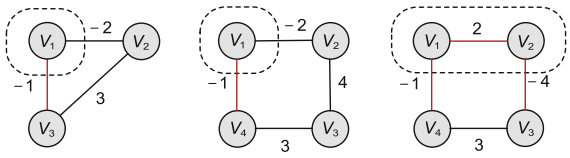

Fig. 3 Graphs of the structurally balanced nodes

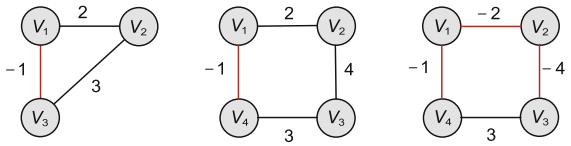

Fig. 4 Graphs of the structurally unbalanced nodes

Based on the privacy-preserving mechanism proposed in this study, a new signed graph is obtained, and the following lemma is proposed to analyze the properties of the graph:

Lemma 1 For an undirected graph $\mathcal{G}$, which is structurally balanced, after Algorithms 1 and 2, the resulting new graph $\bar{\mathcal{G}}$ is still structurally balanced.

Proof The decomposition method adopted in this study is to first decompose each node into n_i sub-nodes, where n_i is the number of neighbor nodes of node v_i, and then connect those sub-nodes after decomposing to form a chain. When judging whether the new topology after decomposition is structurally balanced, because the weight between the homologous nodes is positive, a chain formed by the homologous nodes can be regarded as a node. So, all nodes can be divided into two sets by Definition 1. In addition, the weights $a_i^{s,j}$ between homologous

nodes are positive; therefore, two nodes connected by a negative edge are from different sets. So, after Algorithm 1, the resulting new graph $\bar{\mathcal{G}}$ is still structurally balanced.

The following lemma considers a gauge transformation that creates a link between the average consensus and the bipartite consensus:

Lemma 2 Given scalars $\delta_i \in \{\pm 1\}$, δ_i composes diagonal matrix $\boldsymbol{Q} = \mathrm{diag}_n\{\delta_i\}$. Define a set $\mathbb{Q} = \{\boldsymbol{Q} \mid \boldsymbol{Q} = \mathrm{diag}_n\{\delta_i\}, \delta_i \in \{\pm 1\}\}$, where $\mathbb{Q} \subseteq \mathbb{R}^{n\times n}$. $\boldsymbol{L}$ is the Laplacian matrix of the graph $\mathcal{G}$. $\boldsymbol{A}$ is the adjacency matrix of the graph $\mathcal{G}$, which is a signed graph of system (1) and $\boldsymbol{D}$ is the degree matrix of graph $\mathcal{G}$. When the graph is a structurally balanced graph, there is a diagonal matrix $\boldsymbol{Q} \in \mathbb{Q}$, which makes the elements of $\boldsymbol{QAQ}$ non-negative.

Proof Consider the transformation of coordinates corresponding to the gauge transformation $\boldsymbol{Q}$. Define $\boldsymbol{y}[k] = \boldsymbol{Qx}[k]$. Based on the fact $\boldsymbol{Q} = \boldsymbol{Q}^{-1}$, one has

$$\begin{aligned}\boldsymbol{Q}^{-1}\boldsymbol{y}[k] &= \boldsymbol{Q}^{-1}\boldsymbol{Qx}[k],\\ \boldsymbol{Qy}[k] &= \boldsymbol{x}[k].\end{aligned}$$

Then, substituting the above results into Eq. (3) derives

$$\begin{aligned}\boldsymbol{x}[k+1] =& \boldsymbol{Qy}[k] - \varepsilon(\boldsymbol{D}-\boldsymbol{A})\boldsymbol{Qy}[k],\\ \boldsymbol{Qy}[k+1] =& \boldsymbol{x}[k+1]\\ =& \boldsymbol{Qy}[k] - \varepsilon(\boldsymbol{D}-\boldsymbol{A})\boldsymbol{Qy}[k],\\ \boldsymbol{y}[k+1] =& \boldsymbol{y}[k] - \varepsilon\boldsymbol{Q}(\boldsymbol{D}-\boldsymbol{A})\boldsymbol{Qy}[k]\\ =& \boldsymbol{y}[k] - \varepsilon(\boldsymbol{QDQ}-\boldsymbol{QAQ})\boldsymbol{y}[k]\\ =& \boldsymbol{y}[k] - \varepsilon\boldsymbol{L}_{\boldsymbol{Q}}\boldsymbol{y}[k],\end{aligned}$$

where $\boldsymbol{L}_{\boldsymbol{Q}} = \boldsymbol{D} - \boldsymbol{QAQ} = \boldsymbol{Q}(\boldsymbol{D}-\boldsymbol{A})\boldsymbol{Q} = \boldsymbol{QLQ}$. Along the same line, for the decomposed system (4), there is a diagonal matrix $\boldsymbol{Q} \in \mathbb{Q}$, such that $\boldsymbol{Q}\bar{\boldsymbol{A}}\boldsymbol{Q}$ is non-negative, where $\bar{\boldsymbol{A}}$ is the adjacency matrix of the graph $\bar{\mathcal{G}}$. From Altafini (2013), it can be concluded that $\boldsymbol{L}$ and $\boldsymbol{L}_{\boldsymbol{Q}}$ are isospectral, that is, $\mathrm{sp}(\boldsymbol{L}) = \mathrm{sp}(\boldsymbol{L}_{\boldsymbol{Q}})$.

The following example illustrates a gauge transformation:

Example 1 To easily explain the gauge transformation, we provide the following example as shown in Figs. 5 and 6. The meanings represented by edges of different colors are the same as those in Figs. 1 and 2.

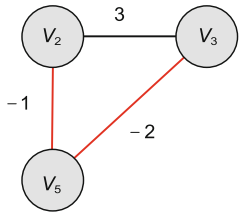

Fig. 5 Weighted symbol graph of three nodes. References to color refer to the online version of this figure

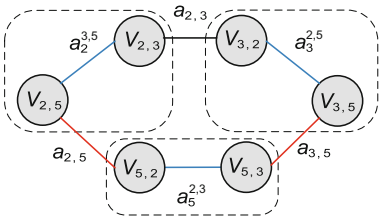

Fig. 6 Weighted symbol graph after decomposition. References to color refer to the online version of this figure

The adjacency matrix $\bar{\boldsymbol{A}}$ of Fig. 6 is

$$\bar{\boldsymbol{A}} = \begin{pmatrix} 0 & a_2^{3,5} & 3 & 0 & 0 & 0\\ a_2^{3,5} & 0 & 0 & 0 & -1 & 0\\ 3 & 0 & 0 & a_3^{2,5} & 0 & 0\\ 0 & 0 & a_3^{2,5} & 0 & 0 & -2\\ 0 & -1 & 0 & 0 & 0 & a_5^{2,3}\\ 0 & 0 & 0 & -2 & a_5^{2,3} & 0 \end{pmatrix}, \quad (5)$$

where $a_2^{3,5}$, $a_3^{2,5}$, and $a_5^{2,3}$ are the weights between homologous nodes after decomposition, $a_i^{r,s} \in (0, \frac{1}{3\varepsilon})$, $i \in \{2,3,5\}$, $r \in \{2,3\}$, and $s \in \{3,5\}$.

Given diagonal matrix $\boldsymbol{Q} = \mathrm{diag}\{1,1,1,1,-1,-1\}$, perform a gauge transformation on the adjacency matrix $\bar{\boldsymbol{A}}$; that is, if $\boldsymbol{Q}\bar{\boldsymbol{A}}\boldsymbol{Q}$ is a matrix with all non-negative elements, then the signed graph can be transformed into a graph with all positive nodes. In this sense, the general bipartite consensus problem can be transformed into an average consensus problem.

Next, we are going to present theorems to demonstrate that based on the node decomposition Algorithms 1 and 2, the decomposed system (4) can attain bipartite consensus while ensuring the confidentiality of the initial node values from honest-but-curious nodes and eavesdroppers.

3 Bipartite consensus analysis

Using the definitions and lemmas introduced in Section 2, we analyze the bipartite consensus of the sub-node states after Algorithms 1 and 2.

Theorem 1 For the cooperative–competitive multi-agent system (4) with a connected signed graph $\bar{\mathcal{G}}(\bar{\boldsymbol{A}})$, if graph $\bar{\mathcal{G}}(\bar{\boldsymbol{A}})$ is structurally balanced, the bipartite solution of Eq. (4) satisfies $\lim\limits_{k\to\infty}\boldsymbol{x}[k]=\frac{1}{2N}\left(\mathbf{1}^{\mathrm{T}}\boldsymbol{Q}\boldsymbol{x}[0]\right)\boldsymbol{Q}\mathbf{1}$, where $\boldsymbol{Q}$ is a diagonal matrix in Lemma 2; if graph $\bar{\mathcal{G}}(\bar{\boldsymbol{A}})$ is structurally unbalanced, then $\lim\limits_{k\to\infty}\boldsymbol{x}[k]=\mathbf{0}$ for $\forall\boldsymbol{x}_i[0]\in\mathbb{R}^{n_x}$.

Proof First, because the original graph $\mathcal{G}$ is a connected graph, the graph $\bar{\mathcal{G}}$ is also a connected graph by the use of the decomposition mechanism of Algorithm 1. In this sense, define the adjacency matrix of graph $\bar{\mathcal{G}}$ as $\bar{\boldsymbol{A}}(k)$. Because the graph $\bar{\mathcal{G}}$ is a connected graph, the adjacency matrix $\bar{\boldsymbol{A}}(k)$ is irreducible.

Second, through the privacy-preserving mechanism proposed in Algorithms 1 and 2, we can obtain $2N$ nodes. Considering that $\mathcal{G}$ is a structurally balanced graph, according to Lemma 1, it can be concluded that the topology graph of $\bar{\mathcal{G}}$ is also a structurally balanced graph. According to Definition 1, we can divide these $2N$ nodes into two sets, respectively represented as $\mathcal{V}_1$ and $\mathcal{V}_2$. From Lemma 2, there is a diagonal matrix $\boldsymbol{Q}$ with diagonal elements being ±1. Specifically, in the diagonal matrix $\boldsymbol{Q}$, the symbol of elements corresponding to nodes from different sets $\mathcal{V}_1$ and $\mathcal{V}_2$ are opposite, as in Example 1. After this gauge transformation, each element in $\boldsymbol{Q}\bar{\boldsymbol{A}}\boldsymbol{Q}$ is non-negative, where $\bar{a}_{i,j}$ is an element of $\boldsymbol{Q}\bar{\boldsymbol{A}}\boldsymbol{Q}$ satisfying $0<\bar{a}_{i,j}(k)<\frac{1}{\sqrt{3\varepsilon}}$. In view of this, the topology structure of the cooperative–competitive network can be transformed into a topology network with only positive weights. Therefore, the bipartite consensus problem can be transformed into an average consensus problem.

Next, we are going to specifically deal with the bipartite consensus solution. If $\bar{\mathcal{G}}$ is structurally balanced, according to Olfati-Saber and Murray (2004), system (4) globally asymptotically solves the average consensus problem. So, system (4) has a bipartite consensus solution.

Because $\boldsymbol{Q}\in\mathbb{Q}$, the elements of $\boldsymbol{Q}\bar{\boldsymbol{A}}\boldsymbol{Q}$ are non-negative. According to Lemma 2, one has $\boldsymbol{y}[k]=\boldsymbol{Q}\boldsymbol{x}[k]$, and $\boldsymbol{y}[k+1]=\boldsymbol{y}[k]-\varepsilon\boldsymbol{L}_{\boldsymbol{Q}}\boldsymbol{y}[k]$. Then, regarding the average consensus problem, according to Altafini (2013), one has the following conclusions:

$$\lim_{k\to\infty}\boldsymbol{y}[k]=\frac{1}{2N}(\mathbf{1}^{\mathrm{T}}\boldsymbol{y}[0])\mathbf{1}, \tag{6}$$

$$\lim_{k\to\infty}\boldsymbol{Q}\boldsymbol{x}[k]=\frac{1}{2N}(\mathbf{1}^{\mathrm{T}}\boldsymbol{Q}\boldsymbol{x}[0])\mathbf{1}, \tag{7}$$

$$\lim_{k\to\infty}\boldsymbol{x}[k]=\frac{1}{2N}(\mathbf{1}^{\mathrm{T}}\boldsymbol{Q}\boldsymbol{x}[0])\boldsymbol{Q}\mathbf{1}. \tag{8}$$

So, the state of each node satisfies

$$\lim_{k\to\infty}x_{i,j}[k]=\mathrm{sgn}(\delta_{i,j})\frac{1}{2N}\sum_{p=1}^{n}\sum_{q\in N_i}x_{p,q}[0]. \tag{9}$$

Considering $\sum\limits_{q\in N_p}x_{p,q}[0]=\frac{2N}{n}x_p[0]$, one has

$$\lim_{k\to\infty}x_{i,j}[k]=\mathrm{sgn}(\delta_{i,j})\frac{1}{n}\sum_{p=1}^{n}x_p[0]=\mathrm{sgn}(\delta_{i,j})\bar{x}, \tag{10}$$

where $\bar{x}$ represents the average consensus value attained by system (1).

It can be observed that the bipartite consensus solution attained by system (4) is equal to the average consensus value achieved by system (1).

For a structurally unbalanced graph, there is no matrix $\boldsymbol{Q}$ satisfying the constraint on $\bar{\boldsymbol{A}}(k)$, so $\bar{\boldsymbol{A}}(k)$ has no zero eigenvalue. According to Altafini (2013), the Laplace potential is positive definite, and we have

$$\lim_{k\to\infty}\boldsymbol{x}(k)=\mathbf{0},\ \forall\boldsymbol{x}_i(0)\in\mathbb{R}^{n_x}$$

for $0<a_i^{p,j}[k]<\frac{1}{3\varepsilon}$.

4 Privacy analysis

In this section, we present the privacy analysis for the proposed privacy protection mechanism. Before proceeding, the following definitions are given:

Definition 2 An honest-but-curious node is an agent that correctly follows all protocol steps, but it is curious and collects the received data to understand some information about other participating nodes. An eavesdropper is an external attacker who understands the network topology and is able to eavesdrop on communication links and access exchanged messages (Wang YQ, 2019).

The following is the definition of privacy adopted in this paper:

Definition 3 If an attacker cannot estimate the initial value $x_i[0]$ of node v_i with any guaranteed accuracy, the privacy of node v_i is protected (Wang YQ et al., 2021).

Theorem 2 For the decomposed system (4), an honest-but-curious node v_j cannot infer the initial value $x_i[0]$ of node v_i if node v_i has at least one collaborating node v_m and it is assumed that v_m will not collude with the honest-but-curious node v_j (see Figs. 7 and 8 for an illustrative example).

Proof According to Algorithm 1, agents v_i, v_m, and v_j can be decomposed into sub-nodes. $a_i^{m,j}$ denotes the weight between node $v_{i,j}$ and $v_{i,m}$. Design the weight as follows:

$$\begin{cases} \bar{a}_i^{m,j}[0] = \dfrac{a_i^{m,j}[0](x_{i,m}[0]-x_{i,j}[0])}{\frac{2N}{n}\bar{x}_i[0]-2x_{i,j}[0]}, \\ \bar{a}_m^{i,j}[0] = \dfrac{a_m^{i,j}[0](x_{m,i}[0]-x_{m,j}[0])}{\frac{2N}{n}\bar{x}_m[0]-2x_{m,j}[0]}, \\ \bar{a}_{i,m}[0] = \dfrac{\varepsilon a_{i,m}[0](x_{m,i}[0]-x_{i,m}[0])}{\varepsilon(\frac{2N}{n}\vec{x}[0]-x_{m,j}[0]+x_{i,j}[0])} \\ \qquad\quad + \dfrac{x_{i,m}[0]-\bar{x}_i[0]+x_{i,j}[0]}{\varepsilon(\frac{2N}{n}\vec{x}[0]-x_{m,j}[0]+x_{i,j}[0])}, \\ \bar{a}_i^{p,q} = a_i^{p,q},\ p,q \neq m,j, \\ \bar{a}_m^{p,q} = a_m^{p,q},\ p,q \neq i,j, \\ \bar{a}_j^{p,q} = a_j^{p,q},\ v_p, v_q \in N_j, \\ \bar{a}_{p,q} = a_{p,q},\ p,q \neq i,m, \end{cases} \tag{11}$$

where $\vec{x}[0] \triangleq x_i[0] + x_m[0] - 2\bar{x}_i[0]$.

The line of the proof is to change the initial value $x_i(0)$ of node v_i to $\bar{x}_i(0)$ in system (1), and design the weights between homologous agents decomposed by node v_i in system (4). Then, calculate the information obtained by honest-but-curious node v_j to test whether honest-but-curious node v_j can pry into the privacy of node v_i. If node v_j receives the same information regardless of whether the initial value of node v_i is changed, it indicates that the initial value of node v_i can be protected through the privacy-preserving mechanism.

Design the changed state $\bar{x}_i(0)$ in system (1) as follows:

$$\begin{cases} \bar{x}_i[0] \neq x_i[0], \\ \bar{x}_m[0] = x_i[0] + x_m[0] - \bar{x}_i[0], \\ \bar{x}_p[0] = x_p[0] \quad p \neq i,m. \end{cases} \tag{12}$$

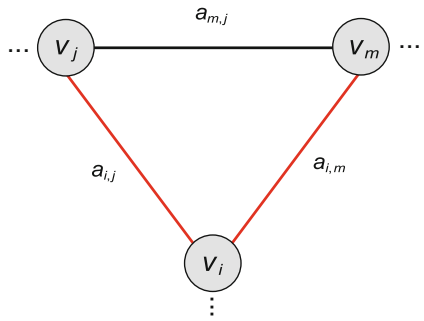

Fig. 7 The original topological structure

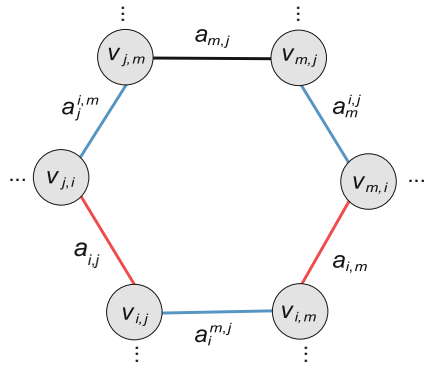

Fig. 8 Topological graph of the original structure decomposed by Algorithm 1

It can be concluded from $\sum_{q\in N_i} x_{i,q}[0] = \frac{2N}{n}x_i[0]$ that

$$\begin{cases} \bar{x}_{i,p}[0] = x_{i,p}[0],\ p \neq m,\ p \in N_i, \\ \bar{x}_{i,m}[0] = \dfrac{2N}{n}\bar{x}_i[0] - \sum\limits_{\substack{p\neq m,\\ p\in N_i}} x_{i,p}[0], \\ \bar{x}_{m,p}[0] = x_{m,p}[0],\ p \neq i, \quad p \in N_m, \\ \bar{x}_{m,i}[0] = \dfrac{2N}{n}\bar{x}_m[0] - \sum\limits_{\substack{p\neq i,\\ p\in N_m}} x_{m,p}[0], \\ \bar{x}_{q,p}[0] = x_{q,p}[0],\ q \neq i,m,\ p \in N_q. \end{cases} \tag{13}$$

In the following, we shall simplify the model and consider only the sub-nodes that are connected to sub-nodes of v_i, v_m, and v_j, including $v_{i,j}, v_{i,m}, v_{m,i}, v_{m,j}, v_{j,m}$, and $v_{j,i}$. $a_{i,j}$ is the weight between node v_i and node v_j. To this end, the weights and the states of Eqs. (11)–(13) can be

rewritten as

$$\begin{cases} \bar{x}_{i,m}[0] = \dfrac{2N}{n}\bar{x}_i[0] - x_{i,j}[0], \\ \bar{x}_{i,j}[0] = x_{i,j}[0], \\ \bar{x}_{m,i}[0] = \dfrac{2N}{n}\bar{x}_m[0] - x_{m,j}[0], \\ \bar{x}_{m,j}[0] = x_{m,j}[0], \\ \bar{x}_{j,i}[0] = x_{j,i}[0], \\ \bar{x}_{j,m}[0] = x_{j,m}[0], \end{cases} \tag{14}$$

and

$$\begin{cases} \bar{a}_i^{m,j}[0] = \dfrac{a_i^{m,j}[0](x_{i,m}[0] - x_{i,j}[0])}{\frac{2N}{n}\bar{x}_i[0] - 2x_{i,j}[0]}, \\ \bar{a}_m^{i,j}[0] = \dfrac{a_m^{i,j}[0](x_{m,i}[0] - x_{m,j}[0])}{\frac{2N}{n}\bar{x}_m[0] - 2x_{m,j}[0]}, \\ \bar{a}_{i,m}[0] = \dfrac{\varepsilon a_{i,m}[0](x_{m,i}[0] - x_{i,m}[0])}{\varepsilon(\frac{2N}{n}\vec{x}[0] - x_{m,j}[0] + x_{i,j}[0])} \\ \qquad\qquad + \dfrac{x_{i,m}[0] - \bar{x}_i[0] + x_{i,j}[0]}{\varepsilon(\frac{2N}{n}\vec{x}[0] - x_{m,j}[0] + x_{i,j}[0])}, \\ \bar{a}_j^{i,m} = a_j^{i,m}, \\ \bar{a}_{i,j} = a_{i,j}, \\ \bar{a}_{m,j} = a_{m,j}. \end{cases} \tag{15}$$

According to Eqs. (14) and (15), we first analyze that the system can achieve privacy protection for an honest-but-curious node. The specific idea is to consider node v_j as an honest-but-curious node in Fig. 7 that wants to peek at the initial value of node v_i. The graph after Algorithm 1 is shown in Fig. 8. When $k = 0$, the information that the honest-but-curious node v_j can receive is defined as

$$\{a_{i,j}[0], x_{i,j}[0], x_{j,i}[0], a_j^{i,m}[0], x_{j,m}[0], a_{m,j}[0], x_{m,j}[0]\}.$$

When $k = 1$, the information that honest-but-curious node v_j can receive is defined as

$$\{a_{i,j}[1], x_{i,j}[1], x_{j,i}[1], a_j^{i,m}[1], x_{j,m}[1], a_{m,j}[1], x_{m,j}[1]\}.$$

Before changing the initial value of node v_i, taking $x_{i,j}[1]$ and $x_{i,m}[1]$ as examples, we illustrate the states of nodes in system (4) as follows:

$$\begin{cases} x_{i,j}[1] = x_{i,j}[0] + \varepsilon|a_{i,j}[0]|(\mathrm{sgn}(a_{i,j})x_{j,i}[0] - x_{i,j}[0]) \\ \qquad\qquad + \varepsilon|a_i^{m,j}[0]|(x_{i,m}[0] - x_{i,j}[0]), \\ x_{i,m}[1] = x_{i,m}[0] + \varepsilon|a_{i,m}[0]|(x_{m,i}[0] - x_{i,m}[0]) \\ \qquad\qquad + \varepsilon|a_i^{m,j}[0]|(x_{i,j}[0] - x_{i,m}[0]). \end{cases} \tag{16}$$

After changing the initial value of node v_i, taking $\bar{x}_{i,j}[1]$ and $\bar{x}_{i,m}[1]$ as examples, illustrate the states of nodes in system (4) as follows:

$$\begin{cases} \bar{x}_{i,j}[1] = \bar{x}_{i,j}[0] + \varepsilon|\bar{a}_{i,j}[0]|(\mathrm{sgn}(\bar{a}_{i,j})\bar{x}_{j,i}[0] - \bar{x}_{i,j}[0]) \\ \qquad\qquad + \varepsilon|\bar{a}_i^{m,j}[0]|(\bar{x}_{i,m}[0] - \bar{x}_{i,j}[0]), \\ \bar{x}_{i,m}[1] = \bar{x}_{i,m}[0] + \varepsilon|\bar{a}_{i,m}[0]|(\bar{x}_{m,i}[0] - \bar{x}_{i,m}[0]) \\ \qquad\qquad + \varepsilon|\bar{a}_i^{m,j}[0]|(\bar{x}_{i,j}[0] - \bar{x}_{i,m}[0]). \end{cases} \tag{17}$$

Substituting Eqs. (14) and (15) to $\bar{x}_{i,j}[1]$ in Eq. (17) yields

$$\begin{aligned} \bar{x}_{i,j}[1] =& \bar{x}_{i,j}[0] + \varepsilon|\bar{a}_{i,j}[0]|(\bar{x}_{j,i}[0] - \bar{x}_{i,j}[0]) \\ & + \varepsilon|\bar{a}_i^{m,j}[0]|(\bar{x}_{i,m}[0] - \bar{x}_{i,j}[0]) \\ =& x_{i,j}[0] + \varepsilon|a_{i,j}[0]|(x_{j,i}[0] - x_{i,j}[0]) \\ & + \varepsilon|\bar{a}_i^{m,j}[0]|(\bar{x}_{i,m}[0] - x_{i,j}[0]) \\ =& x_{i,j}[0] + \varepsilon|a_{i,j}[0]|(x_{j,i}[0] - x_{i,j}[0]) \\ & + \frac{a_i^{m,j}[0](x_{i,m}[0] - x_{i,j}[0])}{\frac{2N}{n}\bar{x}_i[0] - 2x_{i,j}[0]}(\bar{x}_{i,m}[0] - x_{i,j}[0]) \\ =& x_{i,j}[0] + \varepsilon|a_{i,j}[0]|(x_{j,i}[0] - x_{i,j}[0]) \\ & + \frac{a_i^{m,j}[0](x_{i,m}[0] - x_{i,j}[0])}{\bar{x}_{i,m}[0] - x_{i,j}[0]}(\bar{x}_{i,m}[0] - x_{i,j}[0]) \\ =& x_{i,j}[0] + \varepsilon|a_{i,j}[0]|(x_{j,i}[0] - x_{i,j}[0]) \\ & + a_i^{m,j}[0](x_{i,m}[0] - x_{i,j}[0]). \end{aligned} \tag{18}$$

So, we can draw the conclusion $\bar{x}_{i,j}[1] = x_{i,j}[1]$.

Next, we perform a similar proof process for $\bar{x}_{j,i}[1]$. Therefore, we have

$$\begin{aligned} \bar{x}_{j,i}[1] =& \bar{x}_{j,i}[0] + \varepsilon|\bar{a}_{i,j}[0]|(\bar{x}_{i,j}[0] - \bar{x}_{j,i}[0]) \\ & + \varepsilon|\bar{a}_j^{i,m}[0]|(\bar{x}_{j,m}[0] - \bar{x}_{j,i}[0]) \\ =& x_{j,i}[0] + \varepsilon|a_{i,j}[0]|(x_{i,j}[0] - x_{j,i}[0]) \\ & + \varepsilon|a_j^{i,m}[0]|(x_{j,m}[0] - x_{j,i}[0]), \end{aligned} \tag{19}$$

which yields $\bar{x}_{j,i}[1] = x_{j,i}[1]$. Similarly, we can obtain $\bar{x}_{j,m}[1] = x_{j,m}[1]$.

Based on the above derivations, it can be concluded that when $k = 1$ and the initial value of node v_i is changed, the information obtained by honest-but-curious nodes remains unchanged. Next, we shall consider $\bar{x}_{i,m}[1]$ and $\bar{x}_{m,i}[1]$ and prove that the state received by node v_j remains unchanged when $k \geq 2$.

Substituting Eqs. (14) and (15) to $\bar{x}_{i,m}[1]$ in Eq. (17) yields Eq. (20) at the top of the next page.

$$\begin{aligned}\bar{x}_{i,m}[1]=&\bar{x}_{i,m}[0]+\varepsilon|\bar{a}_{i,m}[0]|(\bar{x}_{m,i}[0]-\bar{x}_{i,m}[0])+\varepsilon|\bar{a}_i^{m,j}[0]|(\bar{x}_{i,j}[0]-\bar{x}_{i,m}[0])\\ =&\frac{2N}{n}\bar{x}_i[0]-x_{i,j}[0]+\varepsilon\frac{\varepsilon a_{i,m}[0](x_{m,i}[0]-x_{i,m}[0])+x_{i,m}[0]-\bar{x}_i[0]+x_{i,j}[0]}{\varepsilon(\frac{2N}{n}\vec{x}[0]-x_{m,j}[0]+x_{i,j}[0])}\\ &\cdot\left(\frac{2N}{n}(x_i[0]+x_m[0]-2\bar{x}_i[0])-x_{m,j}[0]+x_{i,j}[0]\right)\\ &+\varepsilon|a_i^{m,j}[0]|(x_{i,j}[0]-x_{i,m}[0])+\varepsilon\frac{a_i^{m,j}[0](x_{i,m}[0]-x_{i,j}[0])}{\frac{2N}{n}\bar{x}_i[0]-2x_{i,j}[0]}\left(x_{i,j}[0]-\frac{2N}{n}\bar{x}_i[0]+x_{i,j}[0]\right)\\ =&x_{i,m}[0]+\varepsilon|a_{i,m}[0]|(x_{m,i}[0]-x_{i,m}[0])+\varepsilon|a_i^{m,j}[0]|(x_{i,j}[0]-x_{i,m}[0]).\end{aligned}\tag{20}$$

So, we derive $\bar{x}_{i,m}[1]=x_{i,m}[1]$. Similarly, it can be concluded that $\bar{x}_{m,i}[1]=x_{m,i}[1]$.

In summary, by designing weights $a_i^{m,j}[0]$, $a_m^{i,j}[0]$, and $a_{i,m}[0]$, starting from $k=1$, the state of each sub-node obtained by decomposing node v_i and node v_m under the alternative initial values $\bar{x}_{i,j}[0]$, $\bar{x}_{j,i}[0]$, $\bar{x}_{j,m}[0]$, $\bar{x}_{m,j}[0]$, $\bar{x}_{i,m}[0]$ will be the same as those under the original initial values $x_{i,j}[0]$, $x_{j,i}[0]$, $x_{j,m}[0]$, $x_{m,j}[0]$, $x_{i,m}[0]$. Therefore, under the two different initial value conditions, all coupling weights can be the same starting from $k=1$. The proof is thus complete.

Remark 2 In the signed network with n nodes, only the weights between homologous child nodes of v_i and the weights of nodes v_m, which can cooperate with node v_i, need to be designed. So, we just need to change weights $a_i^{m,j}[0], a_m^{i,j}[0]$, and $a_{i,m}[0]$. For an honest-but-curious node, the weight consists of two parts: the weight derived from its own interactions with neighbors and the weight among the homologous sub-nodes that it decomposes. It is assumed that node v_m will not collude with node v_j. Therefore, when we change the state $x_i(0)$, it needs to satisfy $\bar{x}_i(0)+\bar{x}_m(0)=x_i(0)+x_m(0)$.

Theorem 3 For the decomposed system (4), eavesdroppers cannot infer the initial value $x_i[0]$ of node v_i if node v_i has at least one collaborating node v_m, which will not collude with eavesdroppers.

Proof Similar to the proof of Theorem 2, without losing generality, consider the cooperative–competitive multi-agent system (see Figs. 7 and 8 for an illustrative example). Because external eavesdroppers cannot obtain the weights between nodes of the same origin (i.e., $a_i^{m,j}$, $a_m^{i,j}$, and $a_{i,m}$), external eavesdroppers cannot calculate the states $x_{i,j}[0]$ and $x_{i,m}[0]$ of the sub-nodes of node v_i, let alone the value of $x_i[0]$. Therefore, eavesdroppers cannot obtain the initial value of node v_i. The proof is complete.

5 Numerical simulations

In this section, two numerical simulation examples are given to demonstrate that the privacy-preserving mechanism can prevent privacy leakage.

Example 2 Consider a multi-agent system with six nodes, where the signed graph is shown in Fig. 1. The initial values are designed as $\boldsymbol{x}(0)=[0.5,3.5,4.6,7.2,4.6,3.6]^{\mathrm{T}}$. The adjacency matrix is

$$\boldsymbol{A}=\begin{pmatrix}0&1&0&-1&0&0\\1&0&1&0&-1&0\\0&1&0&0&-1&0\\-1&0&0&0&1&0\\0&-1&-1&1&0&1\\0&0&0&0&1&0\end{pmatrix}.\tag{21}$$

Due to the presence of seven edges in the topology graph of Fig. 1, these six nodes are decomposed into 2×7 nodes using Algorithm 1 as shown in Fig. 2. According to Theorem 2, the weight between homologous nodes is 0.2, whereas the weight design between non-homologous nodes remains unchanged.

The value of ε is 0.25. Based on the privacy-preserving mechanism, the initial value design of the child nodes after node v_i decomposition means that the sum of the initial values of homologous nodes is $x_i[0]\times\frac{2N}{n}$. $\frac{2N}{n}$ ensures that the bipartite consensus solutions before and after decomposition are equal, that is, $x_i[0]\times\frac{14}{6}$. For example, $x_{2,1}[0]+x_{2,3}[0]+x_{2,5}[0]=3.5\times\frac{14}{6}$. The initial state

after node decomposition is set to

$$\begin{cases} x_{1,2}[0], x_{2,1}[0], x_{2,3}[0], x_{3,2}[0], x_{5,2}[0], x_{4,1}[0], \\ x_{5,3}[0], x_{5,4}[0] \in (0,2), \\ x_{1,4}[0] = 0.5 \times \dfrac{7}{3} - x_{1,2}[0], \\ x_{2,5}[0] = 3.5 \times \dfrac{7}{3} - x_{2,1}[0] - x_{2,3}[0], \\ x_{3,5}[0] = 4.6 \times \dfrac{7}{3} - x_{3,2}[0], \\ x_{4,5}[0] = 7.2 \times \dfrac{7}{3} - x_{4,1}[0] \\ x_{6,5}[0] = 3.6 \times \dfrac{7}{3}, \\ x_{5,6}[0] = 4.6 \times \dfrac{7}{3} - x_{5,2}[0] - x_{5,4}[0] - x_{5,3}[0]. \end{cases}$$

Based on Mo and Murray (2017), at time k, each agent generates a standard normal distributed random variable $m_i[k]$ with mean 0 and variance 1. Assume that all the random variables $m_i[k]_{i=1,2,\ldots,n}, (k = 0, 1, \ldots n)$ are jointly independent. Define $x_i^+[k] = x_i[k] + w_i[k]$, where

$$w_i[k] = \begin{cases} m_i[0], & \text{if} \quad k = 0, \\ \varphi^k m_i[k] - \varphi^{(k-1)} m_i[k-1], & \text{otherwise}, \end{cases}$$

and $0 < \varphi < 1$ is a constant for all agents.

Based on Wang YQ (2019), the evolution law of the external eavesdroppers satisfies

$$\begin{aligned} z[k+1] =& z[k] + x_i^+[k+1] - (x_i^+[k] \\ &+ \varepsilon \sum_{j \in N_i} |a_{i,j}[k]| (\mathrm{sgn}(a_{i,j}[k]) x_j^+[k] - x_i^+[k])). \end{aligned}$$

Due to the unavailability of external eavesdroppers for weights between nodes of the homologous node, the weight between homologous nodes that cannot be accessed by external eavesdroppers is replaced with m. External eavesdroppers randomly assign a value to m between 0 and 5 during calculation.

For example, before applying a privacy-preserving mechanism, external eavesdroppers want to obtain the initial value of node v_1. The external eavesdroppers are set as

$$\begin{aligned} z[k+1] =& z[k] + x_1^+[k+1] - (x_1^+[k] \\ &+ \varepsilon |a_{1,2}[k]| (\mathrm{sgn}(a_{1,2}[k]) x_2^+[k] - x_1^+[k]) \\ &+ \varepsilon |a_{1,4}[k]| (\mathrm{sgn}(a_{1,4}[k]) x_4^+[k] - x_1^+[k])). \end{aligned}$$

After applying a privacy-preserving mechanism, the eavesdropper satisfies the following evolution law, which obtains the initial value of node $v_{1,2}$:

$$\begin{aligned} z[k+1] =& z[k] + x_{1,2}^+[k+1] - (x_{1,2}^+[k] \\ &+ \varepsilon |a_{1,2}[k]| (\mathrm{sgn}(a_{1,2}[k]) x_{2,1}^+[k] - x_{1,2}^+[k]) \\ &+ \varepsilon |m| (\mathrm{sgn}(m) x_{4,1}^+[k] - x_{1,2}^+[k])). \end{aligned}$$

The external eavesdropper cannot obtain the weight between node $v_{1,4}$ and node $v_{1,2}$, so the weight $a_1^{2,4}$ is set as m and $m \in (0, 5)$. Define the initial value of the external eavesdropper as $z[0] = -0.149$.

The corresponding simulation results are shown in Figs. 9–11. From Fig. 9, it can be concluded that the 14 nodes obtained through node decomposition can achieve bipartite consensus, and due to the design of weight, the bipartite consensus solutions before and after decomposition are the same. From Fig. 10, it can be seen that although these six nodes can achieve bipartite consensus before the privacy-preserving mechanism, the initial value of node v_1 can be detected by eavesdroppers without node decomposition. From Fig. 11, it can be observed that through the privacy-preserving mechanism designed in this study, the same eavesdroppers cannot calculate the initial value of node $v_{1,2}$.

Remark 3 This study employs eavesdroppers of the same category as those adopted in Wang YQ (2019). The simulation results reveal that both methodologies achieve privacy preservation while exhibiting fundamental distinctions. Wang YQ (2019) specifically addressed cooperative multi-agent systems, whereas the proposed approach in this study develops distinct algorithms

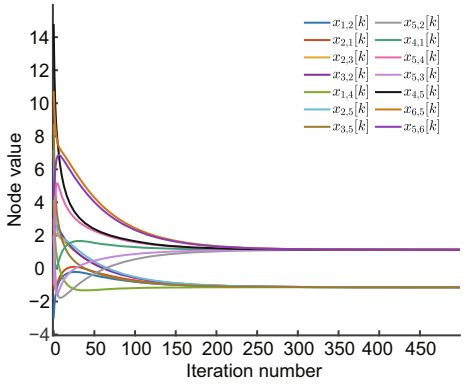

Fig. 9 The bipartite consensus after the node decomposing strategy. The 14 nodes obtained from node decomposition can still achieve bipartite consensus, which is the same as the bipartite consensus before decomposition

tailored for cooperative–competitive multi-agent systems, thereby effectively achieving privacy protection in more complex interactive scenarios.

Example 3 Consider five battery energy storage systems (BESSs) in the microgrid with the interaction topology and Laplacian given in Zhao et al. (2025). For the balancing control problem in Zhao et al. (2025), design the same eavesdropper as in Example 2 as follows:

$$z[k+1] = z[k] + x_i^+[k+1] - (x_i^+[k] + hU[k]),$$

where $x_i^+[k]$ is the same as $x_i^+[k]$ in Example 2, h is a positive scalar, and $U[k]$ is the controller of the system.

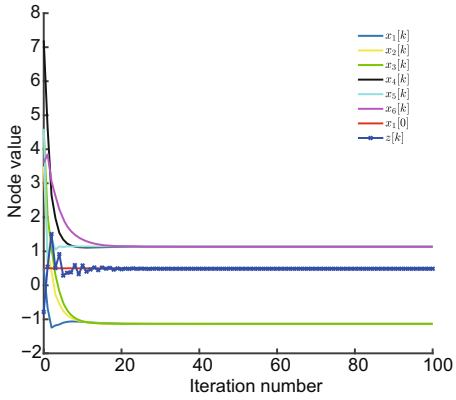

Fig. 10 The bipartite consensus before the privacy-preserving mechanism with the honest-but-curious node. The red horizontal solid line represents the initial value of v_1. Honest-but-curious node z can infer the initial value $x_1[0]$. References to color refer to the online version of this figure

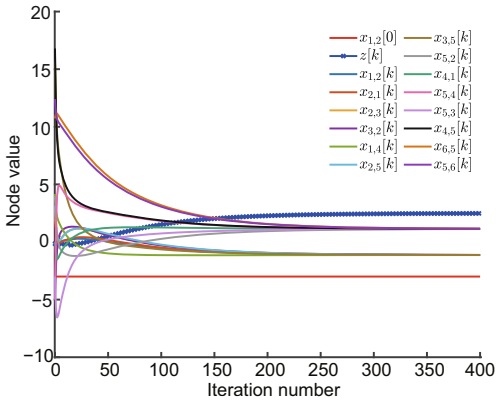

Fig. 11 The bipartite consensus after the privacy-preserving mechanism with the honest-but-curious node. The red horizontal solid line represents the initial value of $v_{1,2}$. Honest-but-curious node z cannot infer the initial value $x_{1,2}[0]$ under Algorithms 1 and 2. References to color refer to the online version of this figure

Without loss of generality, we suppose that an external eavesdropper is interested in obtaining the initial state of BESS 1.

The corresponding simulation results are shown in Figs. 12 and 13. From Fig. 12, it can be concluded that under the eavesdropper in this study, without the privacy-preserving mechanism designed here, the initial states of the BESSs in the original system can be eavesdropped. From Fig. 13, it can be concluded that through the privacy-preserving mechanism designed in this study, when the BESS ceases discharging, the same eavesdropper cannot calculate the initial value of $\mathrm{BESS}_{1,2}$.

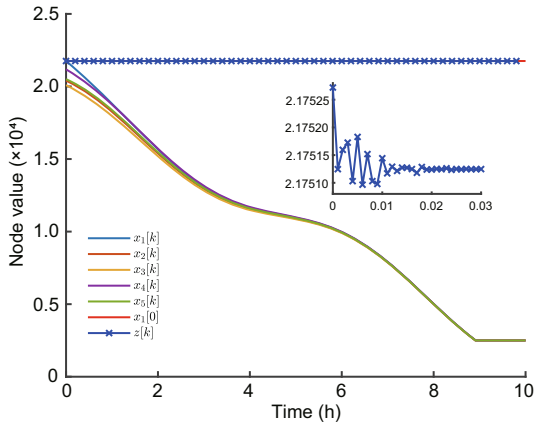

Fig. 12 The bipartite consensus before the privacy-preserving mechanism for BESSs with the eavesdropper. The red horizontal solid line represents the initial value of BESS_1. Eavesdropper z can infer the initial state $x_1[0]$. References to color refer to the online version of this figure

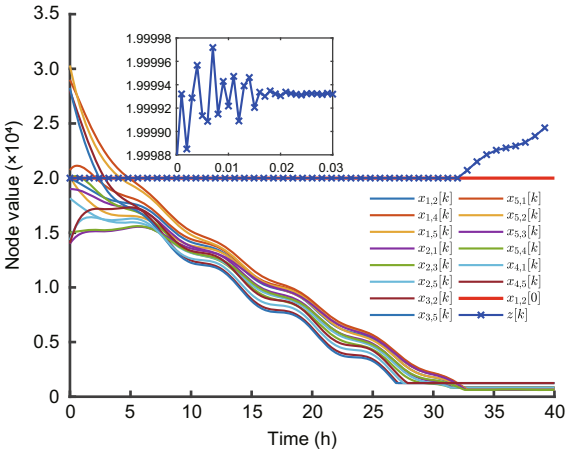

Fig. 13 The bipartite consensus after the privacy-preserving mechanism for BESSs with the eavesdropper. The red horizontal solid line represents the initial value of $\mathrm{BESS}_{1,2}$. Eavesdropper z can infer the initial state $x_{1,2}[0]$. References to color refer to the online version of this figure

6 Conclusions

This study addresses the privacy-protection-based consensus problem for cooperative–competitive multi-agent systems. In undirected signed graphs, a privacy-preserving mechanism has been devised to safeguard node privacy while ensuring bipartite consensus, thus thwarting honest-but-curious nodes and eavesdroppers from accessing the nodes' initial values. The proposed privacy-preserving mechanism encompasses the decomposition mechanism and the weight mechanism. Unlike previous methods of node decomposition, this study shows that through the weight design, privacy protection can be attained without dependence on a third-party algorithm to achieve bipartite consensus. Unlike previous state decomposition methods, after the decomposition mechanism described here, the structurally balanced graph remains structurally balanced. The privacy-preserving mechanism can enable all states of the cooperative–competitive multi-agent system to converge to a bipartite consensus solution, and the initial state of each agent containing sensitive data is privacy-protected. In the end, two numerical simulations have verified the effectiveness of the proposed privacy-protection algorithm. In the future, a potentially interesting direction will be to quantify the maximum information that an adversary can learn under the given model (Li QX et al., 2021).

Contributors

Licheng WANG and Shuai LIU guided the research. Yongling CHEN drafted the paper. All the authors reviewed and finalized the paper.

Conflict of interest

All the authors declare that they have no conflict of interest.

Data availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

References

Altafini C, 2013. Consensus problems on networks with antagonistic interactions. *IEEE Trans Autom Contr*, 58(4):935-946. https://doi.org/10.1109/TAC.2012.2224251

Chanfreut P, Maestre JM, Ferramosca A, et al., 2022. Distributed model predictive control for tracking: a coalitional clustering approach. *IEEE Trans Autom Contr*, 67(12):6873-6880. https://doi.org/10.1109/TAC.2021.3133486

Chen W, Liu L, Liu GP, 2023. Privacy-preserving distributed economic dispatch of microgrids: a dynamic quantization-based consensus scheme with homomorphic encryption. *IEEE Trans Smart Grid*, 14(1):701-713. https://doi.org/10.1109/TSG.2022.3189665

Chen XM, Huang LY, Ding KM, et al., 2023. Privacy-preserving push-sum average consensus via state decomposition. *IEEE Trans Autom Contr*, 68(12):7974-7981. https://doi.org/10.1109/TAC.2023.3256479

Cheng HQ, Liao XF, Li HQ, et al., 2024. Privacy-preserving push-pull method for decentralized optimization via state decomposition. *IEEE Trans Signal Inform Process Netw*, 10:513-526. https://doi.org/10.1109/TSIPN.2024.3402430

Dou J, Song Y, 2023. An improved generative adversarial network with feature filtering for imbalanced data. *Int J Netw Dyn Intell*, 2(4):100017. https://doi.org/10.53941/ijndi.2023.100017

Fang WH, Shen B, Pan AQ, et al., 2024. A cooperative stochastic configuration network based on differential evolutionary sparrow search algorithm for prediction. *Syst Sci Contr Eng*, 12(1):2314481. https://doi.org/10.1080/21642583.2024.2314481

Gao H, Zhang CL, Ahmad M, et al., 2018. Privacy-preserving average consensus on directed graphs using push-sum. IEEE Conf on Communications and Network Security, p.1-9. https://doi.org/10.1109/CNS.2018.8433217

Gao PX, Jia CQ, Zhou AZ, 2024. Encryption–decryption-based state estimation for nonlinear complex networks subject to coupled perturbation. *Syst Sci Contr Eng*, 12(1):2357796. https://doi.org/10.1080/21642583.2024.2357796

Hoseinpour M, Hoseinpour M, Haghifam M, et al., 2024. Privacy-preserving and approximately truthful local electricity markets: a differentially private VCG mechanism. *IEEE Trans Smart Grid*, 15(2):1991-2003. https://doi.org/10.1109/TSG.2023.3301174

Huang J, 2024. Adaptive output synchronization for a class of uncertain nonlinear multi-agent systems over switching networks. *IEEE Trans Autom Contr*, 69(4):2645-2651. https://doi.org/10.1109/TAC.2023.3334992

Jiang Y, Liu L, Feng G, 2024. Fully distributed adaptive control for output consensus of uncertain discrete-time linear multi-agent systems. *Automatica*, 162:111531. https://doi.org/10.1016/j.automatica.2024.111531

Kefayati M, Talebi MS, Khalaj BH, et al., 2007. Secure consensus averaging in sensor networks using random offsets. IEEE Int Conf on Telecommunications and Malaysia Int Conf on Communications, p.556-560. https://doi.org/10.1109/ICTMICC.2007.4448699

Li CY, Liu YF, Gao M, et al., 2024. Fault-tolerant formation consensus control for time-varying multi-agent systems

with stochastic communication protocol. *Int J Netw Dyn Intell*, 3(1):100004. https://doi.org/10.53941/ijndi.2024.100004

Li QX, Cascudo I, Christensen MG, 2019. Privacy-preserving distributed average consensus based on additive secret sharing. 27th European Signal Processing Conf, p.1-5. https://doi.org/10.23919/EUSIPCO.2019.8902577

Li QX, Heusdens R, Christensen MG, 2020. Convex optimisation-based privacy-preserving distributed average consensus in wireless sensor networks. IEEE Int Conf on Acoustics, Speech and Signal Processing, p.5895-5899. https://doi.org/10.1109/ICASSP40776.2020.9053348

Li QX, Gundersen JS, Heusdens R, et al., 2021. Privacy-preserving distributed processing: metrics, bounds and algorithms. *IEEE Trans Inform Forensics Secur*, 16:2090-2103. https://doi.org/10.1109/TIFS.2021.3050064

Liang YP, Tian LL, Zhang X, et al., 2024. Multi-dimensional adaptive learning rate gradient descent optimization algorithm for network training in magneto-optical defect detection. *Int J Netw Dyn Intell*, 3(3):100016.

Liu JH, Long QF, Liu RP, et al., 2024. Privacy-preserving peer-to-peer energy trading via hybrid secure computations. *IEEE Trans Smart Grid*, 15(2):1951-1964. https://doi.org/10.1109/TSG.2023.3293549

Ma JY, Hu JP, 2022. Safe consensus control of cooperative–competitive multi-agent systems via differential privacy. *Kybernetika*, 58(3):426-439.

Mi W, Luo L, Zhong SM, 2023. Fixed-time consensus tracking for multi-agent systems with a nonholomonic dynamics. *IEEE Trans Autom Contr*, 68(2):1161-1168. https://doi.org/10.1109/TAC.2022.3148312

Mo YL, Murray RM, 2017. Privacy preserving average consensus. *IEEE Trans Autom Contr*, 62(2):753-765. https://doi.org/10.1109/TAC.2016.2564339

Olfati-Saber R, Murray RM, 2004. Consensus problems in networks of agents with switching topology and time-delays. *IEEE Trans Autom Contr*, 49(9):1520-1533. https://doi.org/10.1109/TAC.2004.834113

Sakthivel R, Parivallal A, Kwon OM, et al., 2024. Observer-based leader-following cluster consensus for positive multi-agent systems with input time-varying delay. *Int J Syst Sci*, 55(14):3017-3031. https://doi.org/10.1080/00207721.2024.2364294

Sun L, Ding DR, Dong HL, et al., 2024. Privacy-preserving distributed economic dispatch for microgrids based on state decomposition with added noises. *IEEE Trans Smart Grid*, 15(3):2424-2433. https://doi.org/10.1109/TSG.2023.3324138

Sun LC, Wu TJ, Zhang Y, 2023. A defense strategy for false data injection attacks in multi-agent systems. *Int J Syst Sci*, 54(16):3071-3084. https://doi.org/10.1080/00207721.2023.2268239

Talebi MS, Kefayati M, Khalaj BH, et al., 2006. Adaptive consensus averaging for information fusion over sensor networks. IEEE Int Conf on Mobile Ad Hoc and Sensor Systems, p.562-565. https://doi.org/10.1109/MOBHOC.2006.278610

Wang JM, Ke JM, Zhang JF, 2024. Differentially private bipartite consensus over signed networks with time-varying noises. *IEEE Trans Autom Contr*, 69(9):5788-5803. https://doi.org/10.1109/TAC.2024.3351869

Wang LC, Tian EG, Wang CS, et al., 2022. Secure estimation against malicious attacks for lithium-ion batteries under cloud environments. *IEEE Trans Circ Syst I Regul Pap*, 69(10):4237-4247. https://doi.org/10.1109/TCSI.2022.3187725

Wang LC, Wang ZD, Zhao D, et al., 2023. Stabilization of linear discrete-time systems over resource-constrained networks under dynamical multiple description coding scheme. *Automatica*, 156:111160. https://doi.org/10.1016/j.automatica.2023.111160

Wang LC, Wang ZD, Zhao D, et al., 2024. Recursive filtering for discrete-time stochastic complex networks under bit-rate constraints: a locally minimum variance approach. *IEEE Trans Autom Contr*, 69(5):3441-3448. https://doi.org/10.1109/TAC.2023.3349102

Wang LC, Wang ZD, Liu S, et al., 2025. Unscented Kalman filtering over full-duplex relay networks under binary encoding schemes. *IEEE Trans Autom Contr*, 70(5):3441-3448. https://doi.org/10.1109/TAC.2024.3521281

Wang W, Ma LF, Rui QQ, et al., 2024. A survey on privacy-preserving control and filtering of networked control systems. *Int J Syst Sci*, 55(11):2269-2288. https://doi.org/10.1080/00207721.2024.2343734

Wang YQ, 2019. Privacy-preserving average consensus via state decomposition. *IEEE Trans Autom Contr*, 64(11):4711-4716. https://doi.org/10.1109/TAC.2019.2902731

Wang YQ, Lu JQ, Zheng WX, et al., 2021. Privacy-preserving consensus for multi-agent systems via node decomposition strategy. *IEEE Trans Circ Syst I Regul Pap*, 68(8):3474-3484. https://doi.org/10.1109/TCSI.2021.3081372

Wu L, Qin CY, Xu ZH, et al., 2023. TCPP: achieving privacy-preserving trajectory correlation with differential privacy. *IEEE Trans Inform Forensics Secur*, 18:4006-4020. https://doi.org/10.1109/TIFS.2023.3290486

Wu XH, Mu XW, 2022. New design on distributed event-based sliding mode controller for disturbed second-order multiagent systems. *IEEE Trans Autom Contr*, 67(5):2590-2596. https://doi.org/10.1109/TAC.2021.3090754

Yaghoubi Z, Taheri Javan N, Bahaghighat M, 2023. Consensus tracking for a class of fractional-order non-linear multi-agent systems via an adaptive dynamic surface controller. *Syst Sci Contr Eng*, 11(1):2207602. https://doi.org/10.1080/21642583.2023.2207602

Yang P, Freeman RA, Lynch KM, 2008. Multi-agent coordination by decentralized estimation and control. *IEEE Trans Autom Contr*, 53(11):2480-2496. https://doi.org/10.1109/TAC.2008.2006925

Yuan ZP, Li P, Li ZL, et al., 2024. A fully distributed privacy-preserving energy management system for networked microgrid cluster based on homomorphic encryption. *IEEE Trans Smart Grid*, 15(2):1735-1748. https://doi.org/10.1109/TSG.2023.3309405

Zhai SD, Zheng WX, 2019. On survival of all agents in a network with cooperative and competitive interactions. *IEEE Trans Autom Contr*, 64(9):3853-3860. https://doi.org/10.1109/TAC.2019.2892521

Zhang WT, Zuo ZQ, Wang YJ, et al., 2023. How much noise suffices for privacy of multiagent systems? *IEEE Trans Autom Contr*, 68(10):6051-6066. https://doi.org/10.1109/TAC.2022.3232050

Zhao ZY, Tian EG, Wang LC, 2025. Distributed secure balancing control for battery energy storage systems under privacy-preserving mechanisms. *IEEE Trans Autom Sci Eng*, 22:15768-15777. https://doi.org/10.1109/TASE.2025.3571457

Zheng SS, Liu S, Wang LC, 2024. Event-triggered distributed optimization for model-free multi-agent systems. *Front Inform Technol Electron Eng*, 25(2):214-224. https://doi.org/10.1631/FITEE.2300568