Whole-Process Privacy-Preserving and Sybil-Resilient Consensus for Multiagent Networks

Yiming Wu, Chenduo Ying, Ning Zheng, Wen-An Zhang, *Senior Member, IEEE*, and Shanying Zhu, *Senior Member, IEEE*

***Abstract*— This article is concerned with the co-design of privacy-preserving and resilient consensus protocol for a class of multiagent networks (MANs), where the information exchanges over communication networks among the agents suffer from eavesdropping and Sybil attacks. First, we introduce a new attack model in which an adversarial agent could launch a Sybil attack, generating a large number of spurious entities in the network, thereby gaining disproportionate influence. In this communication framework, a whole-process privacy-preserving mechanism is designed that is capable of protecting both initial and current states of agents. Then, instead of existing methods requiring identifying and mitigating Sybil nodes, a degree-based mean-subsequence-reduced (D-MSR) resilient strategy is implemented, showcasing its significant properties: 1) ensuring the effectiveness of aforementioned designed privacy protection strategy; 2) allowing the network to contain Sybil nodes without elimination; and 3) reaching consensus among the normal agents. Finally, several numerical simulations are provided to validate the effectiveness of the proposed results.**

***Index Terms*— Distributed secure control, multiagent networks (MANs), privacy preservation, resilient consensus, Sybil attack.**

I. Introduction

In RECENT years, scholars and engineers have increasingly focused on the secure coordinated problem of multiagent networks (MANs), particularly in situations involving adversaries or misbehaving agents within networks (see, e.g., [1], [2], [3], [4], [5], [6] and the references therein). One of the critical issues is the secure consensus problem, whose goal is to design distributed resilient control strategies and privacy protection methods for multiple agents that ensure agreement among the normal agents, even in the face of network attacks or manipulation by intruders, while simultaneously ensuring that the status information of these agents remains secure.

Within current research concerning resilient consensus, the predominant malicious attack models include denial-of-service (DoS) attacks [7], [8], [9], [10], [11] and deception attacks (also known as false data injection attacks) [12], [13], [14], [15], [16], [17]. In DoS attacks, the adversary sends a large number of access requests to maliciously block communication channels, making the legitimately transmitted information between agents inaccessible. To improve resilience to such attacks, Xu et al. [7] proposed a fully distributed secure protocol, which uniquely prioritizes scalability and robustness in the presence of distributed DoS attacks, ensuring asymptotic consensus for multiagent systems. Besides, the authors in [9], [10], and [11] incorporated event-triggered control methods into the design of resilient consensus protocols for systems under DoS attacks. In the case of deception attacks, the attacker uses counterfeit data or information, thereby replacing the accurate information within the communication networks. In [13], a resilient consensus algorithm against deception attacks with generalized network robustness concept and trusted edges was proposed. Usevitch and Panagou [14] studied the resilient leader–follower consensus for discrete-time multiagent systems under deception attacks.

Recently, a new type of attack known as the Sybil attack (or spoofing) has gradually attracted the attention of researchers in the field of networked systems [18], [19], [20], [21], [22]. In Sybil attacks, misbehaving agents generate numerous false identities, gaining disproportionate network influence. Such a kind of attack can significantly impair MANs, particularly those executing consensus algorithms [18]. However, most of the existing methods against Sybil attacks are based on identifying malicious nodes and subsequently defending them [18], [19], [20], [21], [22]. This requires the accumulation of a large amount of feature data to assist the identification, resulting in such methods requiring a high resource overhead and poor real-time performance. Besides, a necessary precondition for the resilient control algorithms mentioned above against DoS attacks and deception attacks to execute effectively is that the number of malicious agents (or compromised links) in the network is bounded. However, Sybil attacks can replicate malicious entities in the network without restriction, making it difficult to meet this condition, thereby

Received 17 January 2024; revised 30 August 2024; accepted 26 October 2024. Date of publication 5 November 2024; date of current version 9 July 2025. This work was supported in part by the National Natural Science Foundation of China under Grant 62073109 and Grant 62173305 and in part by Zhejiang Provincial Public Welfare Research Project of China under Grant LGF21F020011. *(Corresponding author: Yiming Wu.)*

Yiming Wu and Ning Zheng are with the School of Cyberspace, Hangzhou Dianzi University, Hangzhou 310018, China (e-mail: ymwu@hdu.edu.cn; nzheng@hdu.edu.cn).

Chenduo Ying is with the State Key Laboratory of Industrial Control Technology and the College of Control Science and Engineering, Zhejiang University, Hangzhou 310027, China (e-mail: cdying@zju.edu.cn).

Wen-An Zhang is with the Department of Automation, Zhejiang University of Technology, Hangzhou 310023, China (e-mail: wazhang@zjut.edu.cn).

Shanying Zhu is with the Department of Automation, Shanghai Jiao Tong University, Shanghai 200240, China (e-mail: shyzhu@sjtu.edu.cn).

Digital Object Identifier 10.1109/TNNLS.2024.3488115

causing these existing resilient algorithms to lose their effect. Therefore, the detrimental effects caused by Sybil attacks on consensus algorithms motivate us to analyze and design a novel, lightweight fault-tolerant control strategy. This strategy is aimed at resisting such attacks without requiring specific identification and removal and achieving consensus among the normal agents, who adhere to pre-established control protocols for state updates.

On the other hand, from a privacy perspective, the participating agents may prefer not to disclose their initial or current state values during the communication process to achieve an agreement [23]. For instance, a group of agents may wish to meet at a specific location while keeping their initial locations confidential to other parties for specific reasons [24]. To remedy privacy concerns of MANs during the consensus process, a series of privacy-preserving algorithms were proposed, such as in [25], [26], [27], and [28]. In the earlier work [25], a differential privacy synchronous mechanism was proposed for the consensus problem. The basic idea behind this method is to add a specific variation in random noise to the information shared among agents. However, such method of protecting privacy by adding random noise can introduce errors in the accuracy of the final consensus value. Another commonly adopted method is cryptography, which is capable of encrypting the exchanged state information [28], [29], [30], [31]. However, cryptography-based approaches often lead to a high computational complexity, significantly increasing the resource overhead. Very recently, Wang [32] proposed a new method based on the concept of state decomposition, which ensures the confidentiality of the node information by preserving a segment of state data locally and using the remaining for information exchange between adjacent nodes. This type of method effectively overcomes the problem of high computational overhead faced by cryptographic methods, while ensuring accurate consensus convergence values. However, most of the aforementioned works only provide the protection of the initial value rather than whole-process protection. As the system approaches convergence, the nodes' state information remains highly susceptible to potential leaks.

Another issue for the aforementioned privacy-preserving algorithms is the lack of consideration for malicious attacks in the network. The injection of false data or DoS attacks in the network can easily invalidate these privacy protection methods. Therefore, it is necessary to consider designing appropriate consensus protocol that has both privacy protection capabilities and attack tolerance. So far, there are few investigations for resilient consensus problems under the privacy protection framework. Fiore and Russo [33] integrated differential privacy with resilient consensus within a MAN containing Byzantine agents and presented a distributed algorithm which ensures that a consensus can be reached by nonadversarial agents. Gusrialdi [34] introduced a unified control framework designed to not only ensure resilient leader–follower consensus in the face of deception attacks but also protect the state value of the agents from eavesdroppers. Weng et al. [35] and Zhang et al. [36], respectively, considered the design of a consensus control protocol for joint privacy protection under DoS attacks and deception attacks. Ying et al. [37] considered the privacy-preserving and resilient consensus problem of MANs under multiple cyber attacks, including deception attacks and DoS attacks. Hu et al. [38] investigated the privacy-preserving consensus strategy against the deception attacks for secondary control of microgrids. However, to the best of the authors' knowledge, the existing resilient consensus algorithms [8], [10], [12], [13], [14], [15], [16], including the above-mentioned algorithms [33], [34], [35], [36], [37], [38] that jointly consider privacy protection, cannot effectively resist such Sybil attacks.

Motivated by the above observation, this work aims to develop fully distributed privacy-preserving-based secure consensus control strategies for MANs subject to Sybil attacks. In this article, the following two questions need to be answered: (Q1) How to design a control scheme so that the MANs can achieve fault-tolerant consensus under Sybil attacks? (Q2) How to integrate a privacy protection scheme into the designed control scheme not only ensures the protection of the node's initial state information but also protects the state information of subsequent moments without affecting the control objective. When compared with the existing related works, the main contributions of this article are as follows.

1) A new attack model is proposed from the perspective of distributed control system, which can effectively depict the behavior of Sybil attacks, i.e., a single malicious node can forge a large number of false entities in the graph, thus gaining a disproportionate influence in the network. Compared with the previously established attack models, the new model possesses the capacity to render the majority of the existing resilient consensus protocols invalid. This motivates us to develop new attack resilient scheme and control protocol applicable to such adversarial network environment.
2) To mitigate the effect of Sybil attacks and achieve the consensus, a degree-based mean-subsequence-reduced (D-MSR) resilient protocol is designed. Compared with works in [18], [19], [20], [21], and [22], our method does not need to identify specific Sybil nodes and, thus, more lightweight.
3) A new privacy-preserving mechanism considering protecting the initial and current states of cooperative agents is proposed. Compared with the differentially private-based algorithms [24], [25], [26], [27] and cryptography-based algorithms [28], [29], [30], [31], [39], our proposed algorithm does not require a huge computational resources, yet successfully obtain accurate consensus value. In addition, all the above works only protect the privacy of initial states of the agents, while the method proposed in this article provides protection for agents' states throughout the whole process, thereby further improving the privacy protection capability.

The rest of this article is structured as follows. In Section II, we present some relevant preliminaries and then formulate the problem of interest. In Section III, the co-design of distributed whole-process privacy-preserving mechanism and resilient consensus protocol under Sybil attacks is provided. Some simulations are performed in Section IV to validate the

main results of this article. Finally, the conclusion is made in Section V.

Notations: Let $\mathbb{R}$ and $\mathbb{Z}$ denote the set of real numbers and integers, respectively. The set of integers greater than or equal to some integer r is denoted $\mathbb{Z}_{\geq r}$. Let $\mathcal{A}$ and $\mathcal{B}$ be two sets, then $|\mathcal{A}|$ is the cardinality of set $\mathcal{A}$, and we denote by $\mathcal{A}\cup\mathcal{B}$, $\mathcal{A}\cap\mathcal{B}$, and $\mathcal{A}\setminus\mathcal{B}$ the union, intersection, and difference of the sets, respectively. For any appropriately dimensioned matrix A, A^{T} represents the transpose of A, and $r(A)$ represents the rank of A.

II. Preliminaries and Problem Formation

A. Graph-Related Notions

A weight undirected graph composed of N nodes can be represented by $\mathcal{G}=\{\mathcal{V},\mathcal{E},A\}$, where $\mathcal{V}=\{1,2,\ldots,N\}$ and $\mathcal{E}\subseteq\mathcal{V}\times\mathcal{V}$ indicate the set of nodes and the set of edges in $\mathcal{G}$, respectively. The connectivity between two nodes is denoted by the weight matrix $A=[a_{ij}]\in\mathbb{R}^{N\times N}$. If $(i,j)\in\mathcal{E}$, then we have $(j,i)\in\mathcal{E}$, which denotes that node i can exchange information with node j and $a_{ij}=a_{ji}>0$; otherwise, $a_{ij}=a_{ji}=0$. In this article, we do not consider the node self-loop case, i.e., $a_{ii}=0$. The neighbor set of node i is denoted as $\mathcal{N}_i=\{j\in\mathcal{V}|(j,i)\in\mathcal{E}\}$, and its cardinality, termed as the degree of node i, is denoted by $d_i=|\mathcal{N}_i|$. A time-varying graph is represented by $\mathcal{G}[k]=\{\mathcal{V}[k],\mathcal{E}[k],A[k]\}$ with $k\in\mathbb{Z}_{\geq 0}$ being the time index. Herein, the node set $\mathcal{V}[k]$, edge set $\mathcal{E}[k]$, and adjacency matrix $A[k]$ dynamically change over time.

Based on the graph definitions provided above, to capture the form of information redundancy in a graph, we use the following topological properties named *r-reachable set* and *r-robust graph*, which were proposed in [17] and slightly modified in [12], respectively.

Definition 1 (r-Reachable Set [12]): A nonempty node set $\mathcal{A}\subset\mathcal{V}$ is said to be an r-reachable set if there exists a node $i\in\mathcal{A}$ such that $|\mathcal{N}_i\setminus\mathcal{A}|\geq r$, $r\in\mathbb{Z}_{\geq 0}$.

Definition 2 (r-Robust Graph [12]): A graph $\mathcal{G}$, comprising N nodes ($N\geq 2$), is said to be an r-robust graph if, for every pair of disjoint sets $\mathcal{A}_1$, $\mathcal{A}_2\subset\mathcal{V}$, at least one is r-reachable set.

B. Adversary Model

In this work, two potential threats to MANs are explored: theft of system state information and disruption of system consensus algorithms. To clearly express the impact of the two types of attack intentions mentioned above on the system, we have provided specific corresponding attack models.

1) Eavesdropper Model: Generally speaking, the purpose of an eavesdropper is to steal sensitive information from the system in a concealed manner, and his behavior itself will not interfere with the system's control algorithm. Specifically, using hacking techniques, attackers intrude the system and acquire details of the entire network's topology. They hold the capability to monitor and record the information sent and received by any node within the network, thereby inferring and obtaining the desired private information. According to these behaviors, the definition of network eavesdropper can be defined as follows.

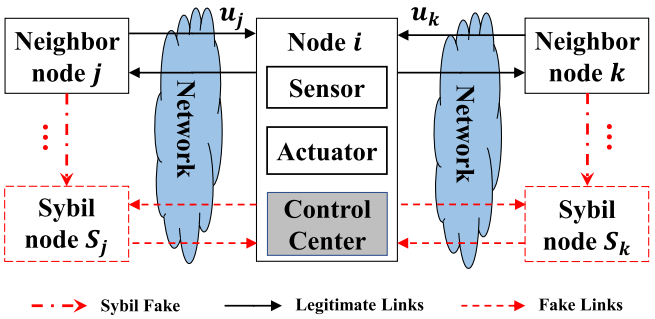


Fig. 1. Illustration of a MAN under Sybil attacks.

Definition 3 (Network Eavesdropper): The network eavesdropper exists in a MAN, who has obtained the entire network's communication topology information, i.e., the adjacency matrix A, and can eavesdrop and record the information transmitted in the edges of any node $i\in\mathcal{V}$ in the network.

2) Sybil Attack Model: Relative to DoS and Byzantine attacks, the research on Sybil attacks in MANs remains limited [2]. In Sybil attacks, some vulnerable nodes in the network generate multiple false mirrors actively under the manipulation of the attacker, while some highly defensive nodes will be passively and unknowingly forged due to the attacker's influence [19], [20]. The primary objective of such actions is to gain the majority of influence within the targeted system, to facilitate its manipulation [18]. Traditional MSR-type resilient algorithms, designed to withstand DoS or Byzantine attacks, typically assume a fixed number of malicious nodes present in the network during algorithm execution. However, in the case of Sybil attacks, the number of malicious nodes (i.e., forged nodes) can dynamically change over time, rendering the aforementioned algorithms ineffective. As a result, the design of resilient consensus algorithms faces greater challenges when dealing with Sybil attacks, compared with DoS or Byzantine attacks. Specifically, Sybil node refers to a type of fake node generated by attackers who compromise normal nodes and clone their identities. The behavior of Sybil node is summarized in the following definition.

Definition 4 (Sybil Node): A node is called the Sybil node if it possesses the following abilities and behaviors.

1) It can obtain all the information of the compromised node, including the messages received and sent out;
2) It has a legitimate identity, that is, it will not be recognized by other normal nodes in the network, so it can establish communication links with the neighbors of the compromised node, and send and receive information with them;
3) It does not obey the prescribed control protocol and will send false information to neighboring nodes.

Fig. 1 gives an illustration of a MAN under Sybil attacks that have been discussed above. The attacker faked the identities of node j and k in the network and created multiple independent Sybil nodes S_j and S_k. The Sybil nodes have all the relevant information of the compromised node. They can establish communication edges with the neighbor node i of

the compromised node and send and receive messages with i. This not only allows them to steal information from normal nodes i, j, and k but also send false information to interfere with nodes i, j, and k. Obviously, a MAN can be maliciously navigated to deviation when there are a large number of Sybil nodes in the network.

C. Problem Formulation

Now, we formulate the problem of interest. We consider a first-order discrete-time MAN consisting of N nodes. Each node i decomposes its state x_i into two substates, x_i^α and x_i^β, and updates its state according to a prescribed control rule as follows:

$$x_i[k] = \begin{cases} (x_i^\alpha[k] + x_i^\beta[k])/2, & k = 1 \\ x_i[k-1] + u_i[k-1], & k > 1 \end{cases} \tag{1}$$

where $k \in \mathbb{Z}$ is the discrete-time index, and $u_i \in \mathbb{R}$ is the control input to be designed.

We consider the existence of eavesdroppers in the network, who are secretly monitoring and collecting interaction information between nodes. If the initial values and current state values of the nodes in MAN cannot be known to such eavesdroppers, then we say the network has achieved whole-process privacy protection (WP-PP). Mathematically, it can be defined as follows.

Definition 5: (*Whole-Process Privacy-Preserving*). We say that a MAN has obtained WP-PP if, for any node $i \in \mathcal{V}$, the initial state value $x_i[0]$ and the current state value $x_i[k]$, $k \geq 1$ cannot be inferred by eavesdroppers with any guaranteed accuracy.

Meanwhile, we consider the case that the network contains normal nodes and Sybil nodes. Let the set $\mathcal{A}$ and set $\mathcal{B}[k]$ denote the normal node set and the Sybil node set, respectively. It is worth noting that the set of normal nodes remains fixed throughout, while the set of Sybil nodes is time-varying due to the characteristic of the Sybil attack model we have constructed. Let $\mathcal{G}[k]$ represent the MAN containing Sybil nodes, and let $x_{\min}[k]$ and $x_{\max}[k]$ denote the minimum and maximum state values of normal nodes $i \in \mathcal{A}$ at time k, respectively. Then, based on the definition of resilient consensus in [12] and [40], the Sybil-resilient consensus is defined as follows.

Definition 6: (*Sybil-Resilient Consensus*). Consider a MAN under Sybil attacks, the network is said to have achieved a Sybil-resilient consensus if, under any initial conditions, for any node $i, j \in \mathcal{A}$, the following two conditions are satisfied.

1) There exists a safety interval ϱ such that all regular nodes' state values satisfy $x_i[k] \in \varrho$, for any $k \geq 0$.
2) There exists a consensus value $x_C \in \varrho$ such that $\lim_{k\to\infty}(x_i[k] - x_C) = 0$, for any $i \in \mathcal{A}$.

Remark 1: Most existing literatures [2], [10], [12], [13], [37] define the safety interval by setting the minimum and maximum values at the initial moments of all the regular nodes as the boundaries of the interval. However, in this article, we did not use such fixed values to define the safety interval. Instead, we adopted a general and universal format. On one hand, this consideration takes into account the differences in the physical limits of nodes set in different scenarios in practical systems. On the other hand, it facilitates the flexibility of designers in the process of designing algorithms such as state-decomposition-based mechanisms for designing the transmission information values.

Remark 2: Compared with the open MAN model studied in [41], [42], and [43], the main difference in our network model is that the normal nodes in our network do not leave or join the network. In other words, the normal nodes remain fixed throughout the entire process, while Sybil nodes can join or leave the network at any time (except for the initial time). This consideration is made to facilitate the analysis within the existing framework of resilient consensus problem. If we were to simultaneously consider the departure or addition of normal nodes to the network, it would introduce entirely new challenges to controller design and even the modeling of resilient consensus problem. This is beyond the scope of this article's discussion.

The main objective of this article is to design a secure control protocol, so that the state values of all the regular nodes can achieve consensus in the presence of Sybil attacks, and meanwhile the state values are never known by eavesdroppers during the execution of the control algorithm.

III. Design of Secure Distributed Controller

In this section, we present the co-design of whole-process privacy-preserving mechanism and resilient consensus control of MAN subject to Sybil attacks, as well as the main results of this article. Before that, we introduce the following assumptions.

Assumption 1: The MAN under consideration in this article is in a secure network environment at time $k \leq 1$, i.e., no Sybil attack is launched during this time interval.

Remark 3: This is a reasonable assumption because in a real scenario, attackers usually need to discover the target and find its vulnerabilities before carrying out the attack, which requires a certain amount of time consumption. Such similar assumption is also adopted in [44] and [45].

Assumption 2: In the MAN considered in this article, the number of Sybil nodes is less than half of the neighboring nodes around each normal node, i.e., there is at least one more normal neighbor node than the Sybil neighbor node.

Remark 4: Considering the limited ability of attackers is a commonly used assumption by researchers in the analysis and design of distributed resilient controllers. There are two main reasons for this: 1) considering the actual situation, the attacker's resources (i.e., the ability to launch an attack) are usually constrained within a limited time and 2) if the attacker's capability is not limited, the design of secure and effective control algorithms becomes extremely difficult and impossible when the majority of nodes in the network are malicious nodes.

A. Design of Whole-Process Privacy-Preserving Mechanism

This section is devoted to the design of the privacy-preserving mechanism for MAN. To address the privacy issues of the initial information and subsequent interaction information of the nodes, we will divide it into

two subproblems and design the corresponding solutions in sequence.

First, privacy preservation of the initial state is addressed. To realize this objective, an improved state decomposition algorithm, inspired by Wang [32], is proposed. The fundamental idea of this algorithm is the decomposition of each node's initial state $x_i[0]$ into two random substates, denoted as $x_i^\alpha[0]$ and $x_i^\beta[0]$. Specifically, the substate values obtained from the initial state may be any real number, conditional on the fulfillment of $x_i[0] = (x_i^\alpha[0]+x_i^\beta[0])/2$. The substate x_i^α mirrors the function of its original node, establishing interaction with the x_j^α substate of its adjacent node j. Conversely, the substate x_i^β remains covert, exclusively communicating with x_i^α, devoid of interaction with neighboring nodes. We incorporate the essence of this algorithm and propose our update rules, as follows:

$$\begin{cases} x_i^\alpha[1] = x_i^\alpha[0] + \sum\limits_{j\in\mathcal{N}_i} a_{ij}[0](x_j^\alpha[0] - x_i^\alpha[0]) \\ \qquad\qquad +a_{i,\alpha\beta}(x_i^\beta[0] - x_i^\alpha[0]) \\ x_i^\beta[1] = x_i^\beta[0] + a_{i,\alpha\beta}(x_i^\alpha[0] - x_i^\beta[0]) \end{cases} \tag{2}$$

in which $a_{i,\alpha\beta}$ is the private coupling weight between the two substates $x_i^\alpha[0]$ and $x_i^\beta[0]$.

Algorithm 1 ISD Algorithm

Input: Node initial state $x_i[0]$
initialize generate $x_i^\alpha[0], x_i^\beta[0]$ with constraints.
transmit $x_i^\alpha[0]$ to neighbors.
for $j \in \mathcal{N}_i$ **do**
  receive $x_j^\alpha[0]$.
  store $I_{\mathcal{N}}^i[0] = \{x_j^\alpha[0] | j \in \mathcal{N}_i\} \to S_i$.
end
update state value $x_i[1]$ via (1) and (2).
Output: $x_i[1]$, $I_{\mathcal{N}}^i[0]$

Remark 5: Compared with [32], our algorithm eliminates the need for a preset parameter ε. In the original algorithm, this parameter is necessary to ensure that $\varepsilon \in (0, (1/\Xi)]$, $\Xi := \max_{i=1,2,\ldots,N} |\mathcal{N}_i|$, which in turn required nodes to acquire global network information before the update rules could be fully distributed. Besides, it is observed that the use of update rules in [32] permeates the entire process of system implementation toward convergence. However, if we only consider the privacy protection of the initial states, it is not necessary to have these update rules involved throughout the entire consensus process. Therefore, our algorithm only operates in the initial steps and is no longer executed in subsequent updates.

The revised version of the state decomposition algorithm is illustrated in Algorithm 1, where S_i denotes the autonomous storage memory of node i.

Now, we are going to discuss how privacy can be preserved during the subsequent interaction of information between network nodes. Inspired by Feng et al. [29], we propose a distributed mechanism for handling the current state values of nodes, which is named as latest state discrepancy (LSD) algorithm. This method revolves around the premise that nodes communicate through discrepant information, termed as state difference. It is denoted by $\Delta_j^i[k] = x_i[k] - x_j[k-1]$, where $\Delta_j^i[k]$ represents the discrepant information transmitted from node i to node j. The LSD algorithm at step time $k \geq 1$ is summarized in Algorithm 2.

Algorithm 2 LSD Algorithm

Input: Node state $x_i[k]$, $I^i[k-1]$
for $j \in \mathcal{N}_i$ **do**
  read $I_{\mathcal{N}}^i[k-1] \leftarrow S_i$.
  if $k = 1$ **then**
    encrypt $\Delta_j^i[1] = x_i[1] - x_j^\alpha[0]$.
  end
  else
    encrypt $\Delta_j^i[k] = x_i[k] - x_j[k-1]$.
  end
  transmit $\Delta_j^i[k]$ to node j.
end
for $j \in \mathcal{N}_i$ **do**
  receive $\Delta_i^j[k]$ from node j.
  if $k = 1$ **then**
    decrypt $x_j[1] = x_i^\alpha[0] + \Delta_i^j[1]$.
  end
  else
    decrypt $x_j[k] = x_i[k-1] + \Delta_i^j[k]$.
  end
  store $x_j[k]$.
end
Output: $I_{\mathcal{N}}^i[k] = \{x_j[k] | j \in \mathcal{N}_i\}$

Finally, we propose a distributed privacy protection algorithm, called the WP-PP algorithm, which combines the ISD algorithm for initial state information and the LSD algorithm for subsequent state information of nodes. Algorithm 3 displays the pseudocode of the WP-PP algorithm.

Algorithm 3 WP-PP Algorithm

Input: Node initial state $x_i[0]$
initialize node i create storage memory S_i.
process ISD$(x_i[0])$ to obtain $x_i[1]$, $I_{\mathcal{N}}^i[0]$.
for $k = 2, 3, 4, \ldots$ **do**
  read $x_i[k-1]$, $I_{\mathcal{N}}^i[k-2] \leftarrow S_i$.
  process $I_{\mathcal{N}}^i[k-1] =$ **LSD**$(x_i[k-1], I^i[k-2])$.
  update state value $x_i[k]$ via (1).
  store $x_i[k]$, $I_{\mathcal{N}}^i[k-1] \to S_i$.
end
Output: Node updated state $x_i[k]$

Remark 6: The core idea of differential privacy is to add noise to shared information [24], [26], [27], [33], [46]. By introducing noise, there is a tradeoff between privacy and accuracy of the results. When a larger amount of noise is added, it is difficult to guarantee the accuracy of the consensus result. On the other hand, when the amount of noise added is smaller, the privacy protection effect is not ideal. Compared with the differentially private algorithm, our

developed decomposition-based algorithm can ensure accurate consensus results.

Theorem 1: Consider MAN (1) over adversarial network with eavesdroppers and Sybil attacks, if each regular agent $i \in \mathcal{A}$ within $\mathcal{G}[k]$ applies the WP-PP algorithm, then its privacy of state value information can be protected through the whole process.

Proof: We first prove the privacy preservation of the initial state. Consider the situation where there is an eavesdropper in the network. For generality, let $x_i[0]$ represent the initial state of node i, which the eavesdropper aims to infer. Upon executing WP-PP algorithm, the initial state $x_i[0]$ can be computed from $x_i^{\alpha}[0] + x_i^{\beta}[0] = 2x_i[0]$. Notably, $x_i^{\alpha}[0]$ is publicly available for iteration. Consequently, deducing the initial state of node i is akin to inferring the value of $x_i^{\beta}[0]$. Let $\mathcal{I}_{\mathrm{e}}^{i}[1]$ denote the set embodying all information about node i that the eavesdropper can gather at $k = 1$, detailed as follows:

$$\mathcal{I}_{\mathrm{e}}^{i}[1] = \left\{x_i^{\alpha}[1]; x_i^{\alpha}[0]; x_j^{\alpha}[0], a_{ij}[0],\, j \in \mathcal{N}_i\right\}.$$

By converting the initial update rule (2), the value of $x_i^{\beta}[0]$ can be calculated by

$$x_i^{\beta}[0] = \frac{1}{a_{i,\alpha\beta}}\left[x_i^{\alpha}[1] - x_i^{\alpha}[0] - \sum_{j\in\mathcal{N}_i} a_{ij}[0]\left(x_j^{\alpha}[0] - x_i^{\alpha}[0]\right)\right] + x_i^{\alpha}[0]. \tag{3}$$

The eavesdropper is capable of attaining all the values that on the right-hand side of (3), with the exception of the coupling weight value $a_{i,\alpha\beta}$. It is excluded because it is situated privately within node i and does not engage in the exchange of external information. Consequently, the eavesdropper is incapable of inferring the value of $x_i^{\beta}[0]$ from (3), thereby being unable to determine the initial value of node i, which proves that the privacy of the initial state $x_i[0]$ is protected.

Next, we prove that WP-PP provides privacy protection for the current state value. In addition, we use $x_i[k]$ to denote the state of node i that the eavesdropper tries to infer. The set of iteration information accessed by eavesdropper at time k, where $k \geq 2$, is

$$\mathcal{I}_{\mathrm{e}}^{i}[k] = \mathcal{I}_{\mathrm{e}}^{i}[1] \bigcup \left\{\bigcup_{k=2}^{k} (\Delta_j^i[k-1], \Delta_i^j[k-1], a_{ij}[k],\, j \in \mathcal{N}_i)\right\}.$$

Based on the collected information set above, eavesdropper wants to infer the state value $x_i(k)$, which is equivalent to solving the following nonhomogeneous linear equation:

$$\acute{A}x = b \tag{4}$$

where $n = 2|\mathcal{N}_i| + 1$,

$$\acute{A} = [\acute{a}_{ij}]_{(n-1)\times n} = \begin{bmatrix} 1 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & \cdots & 1 \end{bmatrix} \tag{5}$$

$$x = \left[x_i[k], x_j[k-1], \ldots, x_j[k+1], \ldots\right]^{\mathrm{T}} \tag{6}$$

$$b = \left[\Delta_j^i(k), \ldots, \Delta_i^j(k), \ldots\right]^{\mathrm{T}}. \tag{7}$$

Since $r(\acute{A}, b) = r(\acute{A}) < n$, (4) has an infinite number of solutions. Therefore, the state value $x_i[k]$ of any agent cannot be estimated with guaranteed accuracy by eavesdroppers.

Based on the above two steps of proof, we know that MAN (1) under WP-PP algorithm can achieve the whole-process privacy preservation. ■

Remark 7: Note that [29] also addresses the issue of privacy preservation throughout the whole process for MAN. However, the proposed algorithm in [29] requires the use of RSA or other public-key cryptography, which limits its practicality for distributed MAN systems with weak computing and communication capabilities of a single agent. Our proposed method, on the other hand, avoids the shortcomings of cryptographic methods. It has very lightweight computational overhead and is not constrained by other third-party secure communication constraints.

B. Design of Sybil-Resilient Consensus Algorithm

The aforementioned mechanism ensures the privacy of both the initial state and subsequent interaction information throughout the entire process. We now present a distributed control algorithm called D-MSR, enabling MANs to achieve resilient consensus even under Sybil attacks.

Algorithm 4 D-MSR Algorithm

Input: Node initial state $x_i[0]$
initialize storage space S_i.
if $k = 1$ **then**
  for $i \in \mathcal{V}$ **do**
    process ISD$(x_i[0])$.
    record node degree $d_i[1]$ in this moment.
  end
end
if $k > 1$ **then**
  for $i \in \mathcal{V}$ **do**
    process LSD$(x_i[k])$.
    record the current node in-degree $d_i[k]$
    if $d_i[k] = d_i[1]$ **then**
      $\mathcal{R}_i[k] = \mathcal{N}_i^B[k]$.
    end
    else
      get the deviation $\zeta_i[k] = d_i[k] - d_i[1]$.
      derive $\mathcal{R}_i[k]$ by deleting the largest $\zeta_i[k]$ messages and the smallest $\zeta_i[k]$ messages from set $\mathcal{N}_i^B[k]$.
    end
  end
end
update node state $x_i[k]$ via (8).
Output: Node updated state $x_i[k]$.

Specifically, each node $i \in \mathcal{A}$ initially uses the security time mentioned in Assumption 1. During this time, node i not only executes ISD algorithm to protect its initial state value but also records its current in-degree value, which we denote as $d_i[1]$. From time $k \geq 2$, the attacker may initiate Sybil attacks, whereby some nodes unknowingly and passively fake their

identities at the behest of the attacker. The attacker stealthily introduces several fake Sybil nodes and forged links into the message interactions across the network. As a result, the regular nodes affected by these Sybil nodes receive additional messages, causing their state update rulers to be confused. In response to this situation, node i begins by sorting all the collected state messages. The difference between the in-degree value at the current time $d_i[k]$ and the in-degree at the initial time $d_i[1]$ is calculated and denoted as $\zeta_i[k]$. Then, node i eliminates both the largest $\zeta_i[k]$ and smallest $\zeta_i[k]$ messages from the sorted set. The set of nodes that have remaining interaction messages is denoted as $\mathcal{R}_i[k]$ and is used for computations involved in participating in the state update. Note that the form of control input $u_i[k-1]$ can be selected as desired; in this article, we choose the controller as follows:

$$u_i[k-1] = h_i \sum_{j\in\mathcal{R}_i[k]} a_{ij}[k-1](x_j[k-1] - x_i[k-1])$$

where $h_i > 0$ is the control gain. Let $\epsilon_{ij}[k-1] := h_i \sum_{j\in\mathcal{R}_i[k]} a_{ij}[k-1]$, the time $k > 1$ part of (1) can be expressed as

$$x_i[k] = (1-\epsilon_{ij}[k-1])x_i[k-1] + \epsilon_{ij}[k-1]x_j[k-1]. \quad (8)$$

We summarize the distributed Sybil-attack resilient consensus control algorithm in Algorithm 4.

Theorem 2: Consider the MAN (1) subject to Sybil attacks. Suppose that Assumptions 1 and 2 hold. If the initial network topology satisfies an r-robust graph, each regular agent $i \in \mathcal{A}$ updates its state with the D-MSR algorithm, and the gain h_i follows the selection strategy $\gamma < h_i a_{ij}[k] < 1, 0 < \gamma < 1, \forall j \in \mathcal{N}_i$, the resilient consensus can be realized, where the safety interval is given as $\varrho = [\min_i x_i[1], \max_i x_i[1]]$.

Proof: First, we show that Condition 1) of Definition 6 holds with ϱ, i.e., $x_i[k] \in [\min_i x_i[1], \max_i x_i[1]]$ for all $k \geq 2$ and $i \in \mathcal{A}$. By the definition of r-robust graph, we know that each node i in the initial network will receive at least r messages from its neighboring nodes. According to Assumption 1, at time $k = 1$, no attack has occurred in the network. Therefore, we can obtain the in-degree of node i at this moment is $d_i[1] = d_i[0] \geq r$. Meanwhile, according to Assumption 2, we know that for node i from time $k \geq 2$, it will receive at most $r-1$ information values from Sybil nodes. We denote $s_i[k]$ as the number of values received from Sybil nodes by node i at time k. Therefore, we have $\zeta_i[k] = d_i[k] - d_i[1] = s_i[k] \leq r-1$. Then, according to Algorithm 4, the current time each node will remove the top $\zeta_i[k]$ largest and smallest state values from the information set collected in this round. After that, the number of remaining values in the set $\mathcal{R}_i[k]$ will be $d_i[k] - 2\zeta_i[k] = d_i[0] - s_i[k] \geqslant r - (r-1) = 1$. This ensures that at least one external information value is involved in the state update of node i. Meanwhile, under the processing mechanism of D-MSR, the remaining message in $\mathcal{R}_i[k]$ will always fall within the interval $[x_{\min}[k-1], x_{\max}[k-1]]$, regardless of whether the fake message received by node i is within the interval $[x_{\min}[k-1], x_{\max}[k-1]]$ or not.

By the gain h_i satisfying $\gamma < h_i a_{ij}[k] < 1$, we know that $\epsilon_{ij}[k-1] > 0$. Let $x_{\min}[k]$ and $x_{\max}[k]$ denote the smallest and largest values of $x_i[k], i \in \mathcal{V}$, respectively, it follows from (8) that

$$\begin{aligned} x_i[k] &= (1-\epsilon_{ij}[k-1])x_i[k-1] + \epsilon_{ij}[k-1]x_j[k-1] \\ &\geq (1-\epsilon_{ij}[k-1])x_{\min}[k-1] \\ &\quad + \epsilon_{ij}[k-1]x_{\min}[k-1] \\ &= x_{\min}[k-1]. \end{aligned}$$

Similarly, under the chosen gain h_i, the right-hand side of (8) forms a convex combination of $x_i[k-1]$ and the values in $\mathcal{R}_i[k]$, and therefore $x_{\min}[k] \geq x_{\min}[k-1]$. We have similar arguments for the regular agents with safety variable $x_i[k] \leq x_{\max}[k-1]$ and $x_{\max}[k] \leq x_{\max}[k-1]$. Combining the above relationships, we obtain that

$$x_{\max}[1] \geq x_{\max}[k-1] \geq x_i[k] \geq x_{\min}[k-1] \geq x_{\min}[1].$$

Thus, based on the definition of safety interval $\varrho = [\min_i x_i[1], \max_i x_i[1]]$, we have $x_i[k] \in \varrho$, for any $k \geq 0$.

In the remaining part of the proof, we strive to establish consensus among the regular nodes, i.e., we show that Condition 2) of Definition 6 holds with our proposed algorithm. From the aforementioned analysis, it is evident that both $x_{\max}[k]$ and $x_{\min}[k]$ are monotonically bounded functions with respect to time k. As time k tends to infinity, it is expected that a definitive maximum state value $x'_{\max}$ and a definitive minimum state value $x'_{\min}$ will eventually be attained. Evidently, consensus among all the regular nodes in the network can be achieved if $x'_{\max} = x'_{\min}$. We prove this by contradiction. Suppose that $x'_{\max} > x'_{\min}$, and further, assume that there exists a constant $\phi_0 > 0$ such that $x'_{\max} - \phi_0 > x'_{\min} + \phi_0$. Let

$$\mathcal{L}_{\max}(k, \Phi) = \{i \in \mathcal{V} \mid x_i[k-1] > x'_{\max} - \Phi\}$$

and

$$\mathcal{L}_{\min}(k, \Phi) = \{i \in \mathcal{V} \mid x_i[k-1] < x'_{\min} + \Phi\}$$

represent the sets of nodes with state values greater than $x'_{\max} - \Phi$ and less than $x'_{\min} + \Phi$ at time $k-1$, respectively. Then one can always choose a suitably small quantity ϕ such that $\phi < (\gamma^n/(1-\gamma^n))\phi_0$, with the constraint $\phi_0 > \phi > 0$. Given a specific time point k_ϕ, we ensure that $x_{\max}[k_\phi - 1] < x'_{\max} + \phi$ and $x_{\min}[k_\phi - 1] > x'_{\min} - \phi$. Since $x_{\max}[k]$ and $x_{\min}[k]$ are monotonically bounded functions, it follows that $x_{\max}[k_\phi - 1 + c] < x'_{\max} + \phi$ and $x_{\min}[k_\phi - 1 + c] > x'_{\min} - \phi$, where $c \in \mathbb{Z}_{\geq 0}$. We also define a recursively generated sequence $\phi_g = \gamma\phi_{g-1} - (1-\gamma)\phi$, where $g \in \mathbb{Z}_{\geq 1}$. It is evident that $\phi_{g-1} > \phi_g$.

We first consider sets $\mathcal{L}_{\max}(k_\phi, \phi_0)$ and $\mathcal{L}_{\min}(k_\phi, \phi_0)$. Under Assumptions 1 and 2, in a MAN that satisfies the condition of an r-robust graph, during the execution of the D-MSR algorithm, after node i receives all the neighbor information at time k_ϕ, it will remove the top $\zeta_i[k_\phi]$ values and the bottom $\zeta_i[k_\phi]$ values from the neighbor set. Based on our previous analysis, the remaining values will all fall within the interval $[x_{\min}[k_\phi - 1], x_{\max}[k_\phi - 1]]$. Without loss of generality, we assume that node i is in the set $\mathcal{L}_{\min}(k_\phi, \phi_0)$. In the worst case, node i can only use one message from $\mathcal{R}_i[k_\phi]$ as update

input. Let j represent the node corresponding to this message. Then, it follows from (8) that

$$\begin{aligned} x_i[k_\phi] &= (1-\epsilon_{ij}[k_\phi-1])x_i[k_\phi-1] \\ &\quad +\epsilon_{ij}[k_\phi-1]x_j[k_\phi-1] \\ &\geq (1-\epsilon_{ij}[k_\phi-1])x_{\min}[k_\phi-1] \\ &\quad +\epsilon_{ij}[k_\phi-1](x'_{\min}+\phi_0) \\ &> (1-\epsilon_{ij}[k_\phi-1])(x'_{\min}-\phi) \\ &\quad +\epsilon_{ij}[k_\phi-1](x'_{\min}+\phi_0) \\ &= x'_{\min}+\epsilon_{ij}[k_\phi-1]\phi_0-(1-\epsilon_{ij}[k_\phi-1])\phi \\ &> x'_{\min}+\gamma\phi_0-(1-\gamma)\phi \\ &= x'_{\min}+\phi_1. \end{aligned} \tag{9}$$

In the case where node i is in set $\mathcal{L}_{\max}(k_\phi,\phi_0)$, it holds that

$$\begin{aligned} x_i[k_\phi] &= (1-\epsilon_{ij}[k_\phi-1])x_i[k_\phi-1] \\ &\quad +\epsilon_{ij}[k_\phi-1]x_j[k_\phi-1] \\ &\leq (1-\epsilon_{ij}[k_\phi-1])x_{\max}[k_\phi-1] \\ &\quad +\epsilon_{ij}[k_\phi-1](x'_{\max}-\phi_0) \\ &< (1-\epsilon_{ij}[k_\phi-1])(x'_{\max}+\phi) \\ &\quad +\epsilon_{ij}[k_\phi-1](x'_{\max}-\phi_0) \\ &= x'_{\max}-\epsilon_{ij}[k_\phi-1]\phi_0+(1-\epsilon_{ij}[k_\phi-1])\phi \\ &< x'_{\max}-\gamma\phi_0+(1-\gamma)\phi \\ &= x'_{\max}-\phi_1. \end{aligned} \tag{10}$$

We now consider the sets $\mathcal{L}_{\max}(k_\phi+1,\phi_1)$ and $\mathcal{L}_{\min}(k_\phi+1,\phi_1)$. Using the aforementioned analysis, it can be deduced that at time k_ϕ, the state value of at least one node in the set $\mathcal{L}_{\max}(k_\phi+1,\phi_1)$ is smaller than $x'_{\max}-\phi_1$, or the state value of at least one node in the set $\mathcal{L}_{\min}(k_\phi+1,\phi_1)$ exceeds $x'_{\min}+\phi_1$. Hence, with the definition of $\mathcal{L}_{\max}(k_\phi+1,\phi_1)$ and $\mathcal{L}_{\min}(k_\phi+1,\phi_1)$, it is easy to check that $|\mathcal{L}_{\max}(k_\phi+1,\phi_1)|+|\mathcal{L}_{\min}(k_\phi+1,\phi_1)|<|\mathcal{L}_{\max}(k_\phi,\phi_0)|+|\mathcal{L}_{\min}(k_\phi,\phi_0)|$.

Finally, we recursively advance c steps in the above analysis process, with $c\leq n$. Note that at least one of the sets $\mathcal{L}_{\max}(k_\phi+c,\phi_c)$ and $\mathcal{L}_{\min}(k_\phi+c,\phi_c)$ is empty. If $\mathcal{L}_{\max}(k_\phi+c,\phi_c)$ is empty, according to the definition of $\mathcal{L}_{\max}(k,\Phi)$, $x_i[k_\phi+c-1]\leq x'_{\max}-\phi_c$. Similarly, if $\mathcal{L}_{\min}(k_\phi+c,\phi_c)$ is empty, then $x_i[k_\phi+c-1]\geq x'_{\min}+\phi_c$. Therefore, if $\phi_c>0$, it contradicts the monotonic convergence of the node's maximum state and minimum state toward $x'_{\max}$ and $x'_{\min}$, respectively. Recalling the premises $0<\gamma<1$ and $\phi<(\gamma^n/(1-\gamma^n))\phi_0$, we have

$$\begin{aligned} 0 &< \gamma^n\phi_0-(1-\gamma^n)\phi\leq\gamma^c\phi_0-(1-\gamma^c)\phi \\ &= \gamma^c\phi_0-(1-\gamma)(1+\gamma+\cdots+\gamma^{c-1})\phi \\ &= \vdots \\ &= \gamma^2\phi_{c-2}-\gamma(1-\gamma)\phi-(1-\gamma)\phi \\ &= \gamma\phi_{c-1}-(1-\gamma)\phi \\ &= \phi_c. \end{aligned}$$

So the contradiction is there. It shows that ϕ_0 must be zero, and we get $x'_{\max}=x'_{\min}$, which completes the proof. ■

Theorem 3: Considering MAN (1) under the presence of eavesdroppers, if the network topology satisfies an r-robust graph and each nodes follow the given D-MSR algorithm for updating their state values, the system will eventually achieve average consensus, i.e.,

$$\lim_{k\to\infty}x_i[k]=\frac{1}{N}\sum_{j=1}^{N}x_j[0]$$

while ensuring WP-PP of the nodes' state values.

Proof: Since the D-MSR algorithm we designed in this article incorporates the WP-PP mechanism, one can use a similar analytical approach as stated in Theorem 1 to easily obtain the proof that the values of node states are fully protected throughout the entire process.

Therefore, we only prove that under the given network topology conditions, the system can ultimately achieve the average consensus. First, we prove that if each node $i\in\mathcal{V}$ within $\mathcal{G}$ applies the update rules specified in (1) and (2), the cumulative state of all the nodes remains consistent after one iteration. At time $k=0$, as node $i\in\mathcal{V}$ decomposes its own initial state $x_i[0]$ into two substates $x_i^\alpha[0]$ and $x_i^\beta[0]$ with predefined constraints, all the nodes in the network perform one iteration according to the update rules (2) and derive $x_i[1]$ from (1). Now, we have

$$\begin{aligned} x_i[1] &= \frac{1}{2}(x_i^\alpha[1]+x_i^\beta[1]) \\ &= \frac{1}{2}\Bigg(x_i^\alpha[0]+x_i^\beta[0]+\sum_{j\in\mathcal{N}_i}a_{ij}[0](x_j^\alpha[0]-x_i^\alpha[0]) \\ &\quad +a_{i,\alpha\beta}(x_i^\beta[0]-x_i^\alpha[0])+a_{i,\alpha\beta}(x_i^\alpha[0]-x_i^\beta[0])\Bigg) \\ &= \frac{1}{2}\Bigg(x_i^\alpha[0]+x_i^\beta[0]+\sum_{j\in\mathcal{N}_i}a_{ij}[0](x_j^\alpha[0]-x_i^\alpha[0])\Bigg). \end{aligned} \tag{11}$$

Let

$$\begin{aligned} \sum_{i=1}^{N}x_i[1] &= \frac{1}{2}\sum_{i=1}^{N}(x_i^\alpha[0]+x_i^\beta[0]) \\ &\quad +\frac{1}{2}\sum_{i=1}^{N}\Bigg(\sum_{j\in\mathcal{N}_i}a_{ij}[0](x_j^\alpha[0]-x_i^\alpha[0])\Bigg). \end{aligned} \tag{12}$$

Recall the definition of undirected graph, we have $a_{ij}[k]=a_{ji}[k],\forall i,j\in\mathcal{V}$ and thus

$$a_{ij}[0](x_j^\alpha[0]-x_i^\alpha[0])=a_{ji}[0](x_j^\alpha[0]-x_i^\alpha[0]). \tag{13}$$

Substituting (13) into (12) and we have

$$\begin{aligned} \sum_{i=1}^{N}x_i[1] &= \frac{1}{2}\sum_{i=1}^{N}(x_i^\alpha[0]+x_i^\beta[0]) \\ &\quad +\frac{1}{2}\sum_{i=1}^{N}\Bigg(\sum_{j\in\mathcal{N}_i}a_{ij}[0](x_j^\alpha[0]-x_i^\alpha[0])\Bigg) \\ &= \frac{1}{2}\sum_{i=1}^{N}(x_i^\alpha[0]+x_i^\beta[0])+0 \\ &= \sum_{i=1}^{N}x_i[0] \end{aligned} \tag{14}$$

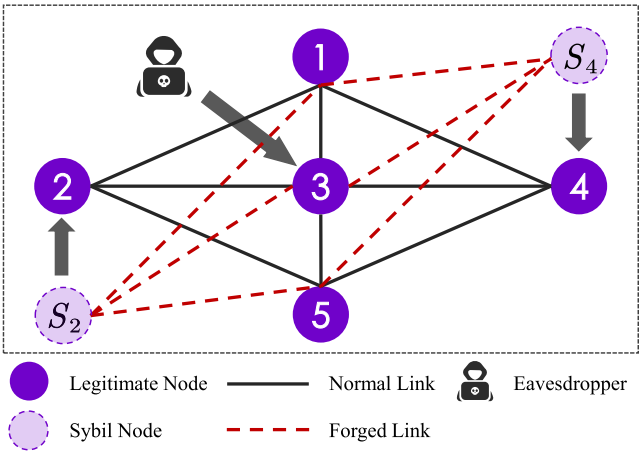


Fig. 2. Topology of the MAN consisting of seven nodes (including five normal nodes and two Sybil nodes).

which implies that the sum of states of all the nodes remains invariant after one iteration update.

According to Lemma 1 in [17], an r-robust graph guarantees a connected network. From time $k = 1$, in the absence of any Sybil nodes, the D-MSR mechanism maintains a constant node in-degree $d_i[k] = d_i[1]$ without discarding any information about its neighboring nodes during the process of state updating, thus ensuring the aforementioned structure of an undirected connected graph. Then, based on the findings of consensus under time-varying weights [47], accurate average consensus can be achieved, i.e., $\lim_{k\to\infty} x_i[k] = \bar{x} = (1/N)\Sigma_{j=1}^{N} x_j[1]$. Further making use of the fact (14) leads to the conclusion that all the node states converge to $(1/N)\Sigma_{j=1}^{N} x_j[0]$. ■

It is worth noting that in Theorem 3, we only consider the presence of eavesdroppers in the MAN. The purpose of this is to verify that the proposed privacy protection mechanism can achieve accurate average consensus without malicious attacks. At the same time, this also indicates that although Sybil attacks cannot disrupt the system's resilient consensus process, they can prevent the system from achieving the accurate average consensus goal.

IV. Simulation Examples

In this section, we use several numerical experiments to validate our theoretical results.

Consider a MAN composed of seven nodes, whose communication topology is depicted in Fig. 2. The initial state of each node corresponds to its serial number, with an array state of $[1, 2, 3, 4, 5]$ and yielding an average value of $x_a[0] = 3$. Each node in the network executes the D-MSR algorithm and has a control gain set to $h_i = 0.125$. To ensure initial state privacy, $a_{i,\alpha\beta}$ is randomly selected from the set of real numbers. The adjacency matrix is selected as a binary matrix, that is, a_{ij} is set to 1 if there is an interaction between nodes and 0 in other cases. Simulations are carried out for both the eavesdropper case and Sybil attack case.

In the first simulation, we assume that the eavesdropper is interested in obtaining the state information of the nodes adjacent to node 3 and constructs the following observer to infer their initial values $x_i[0]$:

$$m_i[k+1] = m_i[k] + x_i[k+1] - (x_i[k] + h_i a_{i3}[k](x_i[k] - x_3[k])) \quad (15)$$

where $m_i[k]$ denotes the value of node i computed by node 3 at time k. Fig. 3 shows the initial state of the neighboring nodes calculated by node 3 and trajectories of MAN with the ISD algorithm. The red dashed line with crosses indicates the calculated value of node 3 over time, and the dashed lines of different colors indicate the initial state of different target nodes. As seen in Fig. 3, the initial states of all the neighboring nodes of node 3 are protected.

Next, we verify the privacy protection capability of each node in the MAN for the current moment's state value. The value observed by an eavesdropper for node i at time k is denoted as $e_i[k]$. Fig. 4 illustrates the trajectories of nodes without the privacy-preserving method for subsequent interaction information. The solid lines of various colors represent the actual state trajectories of each node, while the dashed lines with crosses of different colors represent the eavesdropped state trajectories by the eavesdropper. As illustrated in Fig. 4, when the subsequent interaction information privacy-preserving method is not used, the eavesdropper can directly access the actual node state at any $k \geq 2$. Fig. 5 depicts the MAN trajectories using the proposed LSD method. Evidently, the LSD method efficiently safeguards all subsequent interaction information subsequent to obfuscation of the node's initial state.

The simulation conducted in both the aforementioned groups illustrates that our proposed method effectively prevents the inference of nodes within the MAN network, regardless of their initial state or subsequent interaction information. As a result, privacy is preserved consistently throughout the whole process.

In the second simulation, we illustrate the effectiveness of the D-MSR algorithm for the MAN under Sybil attacks. Considering a scenario where the attacker targets nodes 2 and 4 to instigate Sybil attacks, creating fraudulent Sybil nodes, designated as S_2 and S_4. These Sybil nodes possess complete informational knowledge about their corresponding regular nodes, enabling them to generate forged communication links (represented as red dashed lines) with all the nodes connected to the original node, as illustrated in Fig. 2. Starting from time $k = 2$, the Sybil nodes send extreme values that exceed the safety interval, Namely, $x_{S2}[k] = -2$ and $x_{S4}[k] = 8$, $k \geq 2$, attempting to interfere with the consensus process of adjacent nodes 1, 3, and 5. By running D-MSR algorithm, the trajectories of five regular nodes are shown in Fig. 6, which is evident that each node has successfully achieved resilient consensus. Furthermore, the state value assigned to each node remains encapsulated within the interval $[x_{\min}[1], x_{\max}[1]]$. Further consider the case when the state values of Sybil nodes fall inside $[x_{\min}[1], x_{\max}[1]]$. Here, $x_{S2}[k] = -1$ and $x_{S4}[k] = 6$ are taken as examples. By running the D-MSR algorithm, the trajectories of five normal nodes are shown in Fig. 7, which clearly indicates that network consensus can be achieved but not on average. Note that while it is not

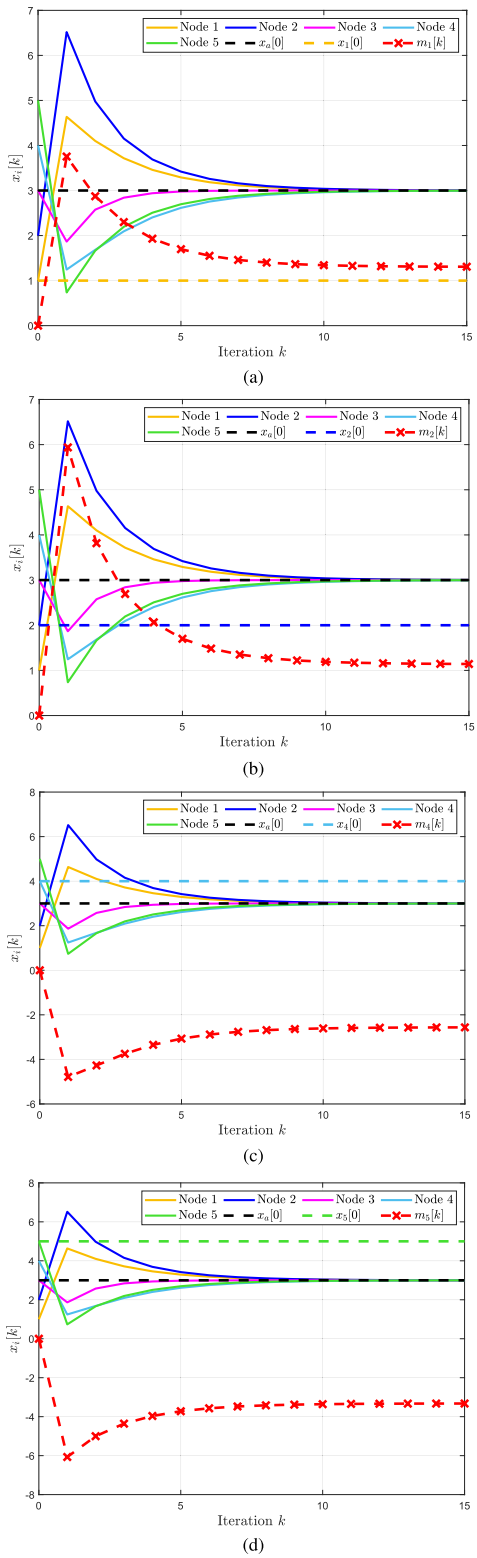


Fig. 3. Trajectory curves of the states of the eavesdropped nodes in the network under ISD algorithm. (a) Eavesdropping target node 1. (b) Eavesdropping target node 2. (c) Eavesdropping target node 4. (d) Eavesdropping target node 5.

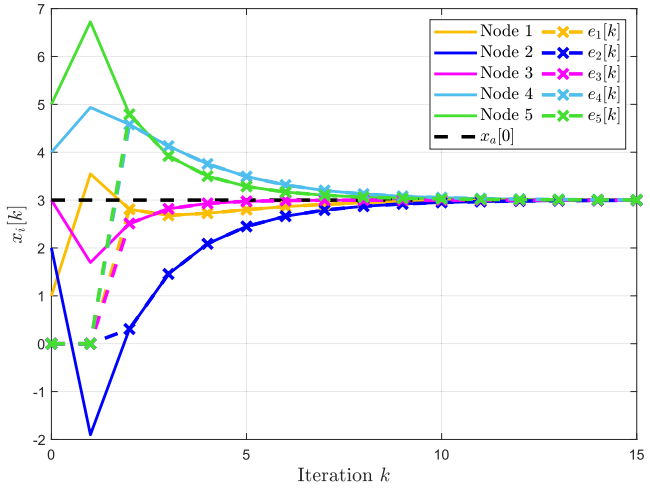


Fig. 4. Trajectory curves of the states of five normal nodes without subsequent interaction information privacy-preserving mechanism.

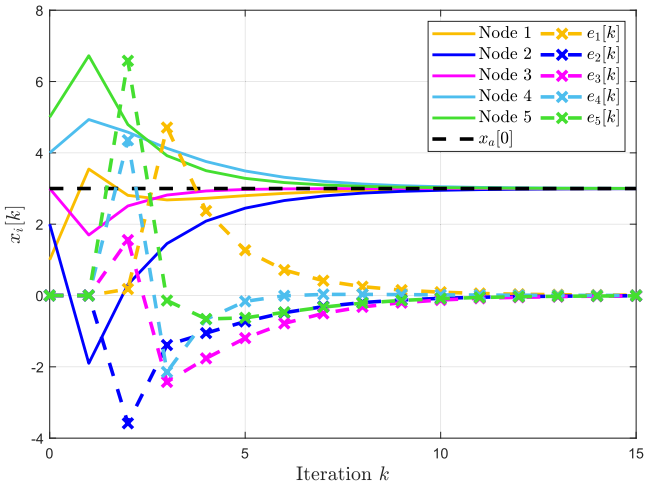


Fig. 5. Trajectory curves of the states of five normal nodes under LSD algorithm.

average consensus, it still conforms to Definition 6, which is Sybil-resilient consensus. No matter whether Sybil nodes send extreme values or values in the safety interval, attackers tend to choose more convenient attack methods for the sake of cost and minimum attack footprint, so we only discuss constant state values here. However, considering variable attacker behavior and state values is a worthy direction for future research.

We then remove links (1, 3) and (3, 5) in Fig. 2, prompting the topology among the agents to no longer meet the conditions for being 3-robust. By applying the definition of a robust graph, it can be discerned that the network topology has transformed into a two-robust graph, a conclusion drawn from inspecting every nonempty disjoint pair of subsets within $\mathcal{V}$. Therefore, according to Theorem 2, we identify that the maximum allowable Sybil node in the current network configuration is one. The trajectories of the five agents are presented in Fig. 8, where the resilient consensus cannot be reached in the network with more than one Sybil node (actually two Sybil nodes).

To evaluate the performance of the proposed algorithm in larger scale MANs, and to compare the computational and communication overhead required by the proposed algorithm with standard consensus algorithm, we considered a MAN

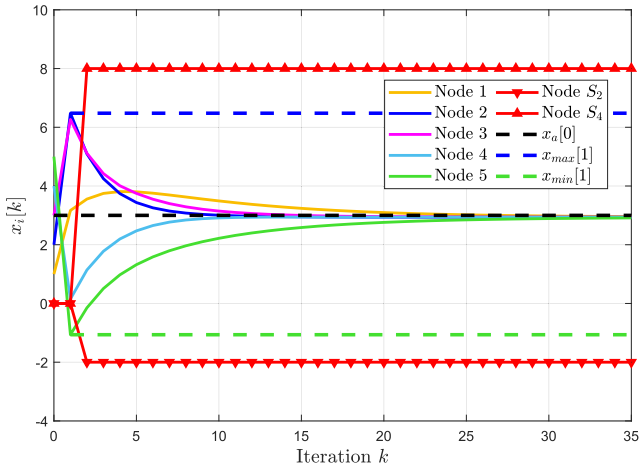


Fig. 6. State trajectories of the nodes in the MAN that satisfies the required network robustness.

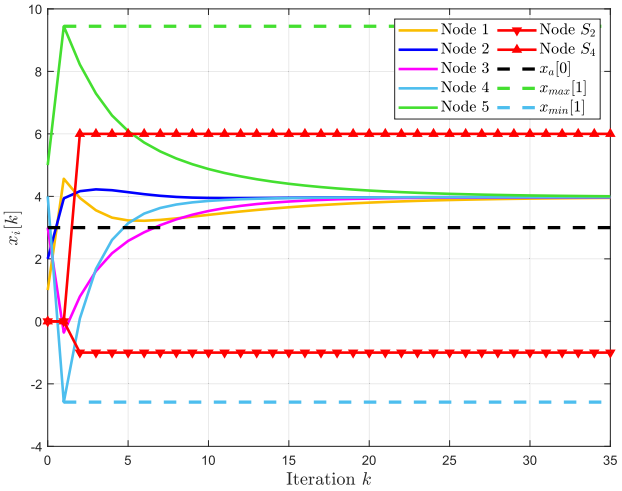


Fig. 7. State trajectories of the nodes in the MAN that Sybil nodes' state value inside $[x_{\min}[1], x_{\max}[1]]$.

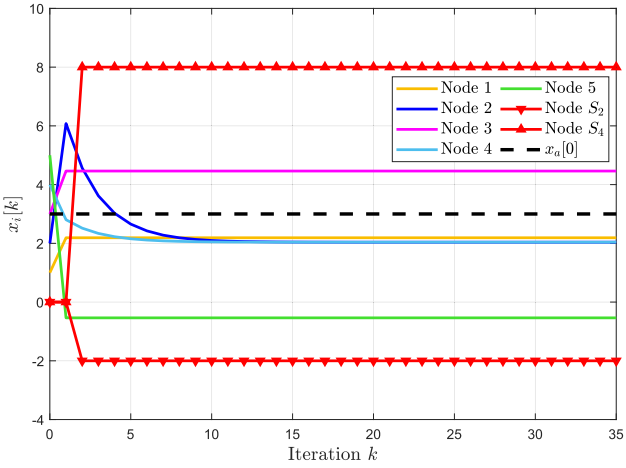


Fig. 8. State trajectories of the nodes in the MAN that do not satisfy the required network robustness.

consisting of 51 nodes, including 49 normal nodes and two Sybil nodes generated by Sybil attacks. The communication topology of the network is shown in Fig. 9, which is constructed based on Theorem 5 in [12] to ensure a 3-robust

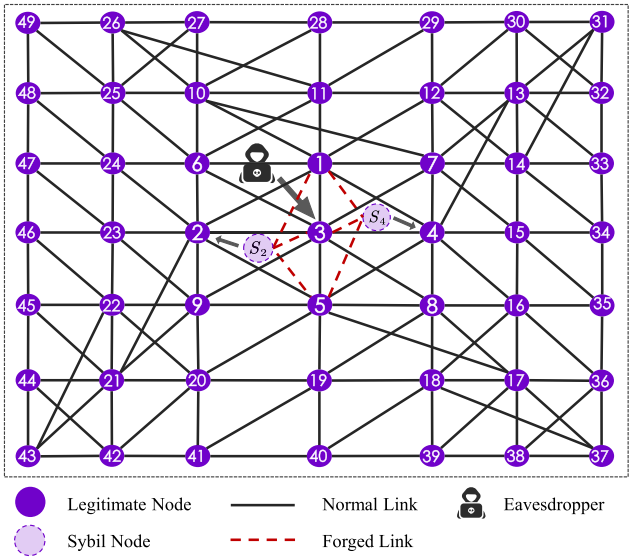


Fig. 9. Topology of the MAN consisting of 51 nodes (including 49 normal nodes and two Sybil nodes).

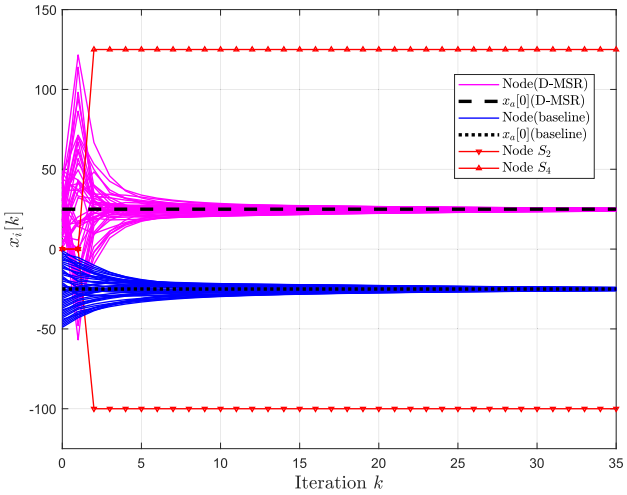


Fig. 10. Overhead comparison between the D-MSR algorithm and baseline consensus algorithm.

communication graph. The normal nodes in the network were updated using the control method proposed in this article, and the final experimental results are shown in Fig. 10. It can be observed that despite the influence of false values sent by Sybil nodes, the states of all the normal nodes in the network eventually reach consensus and converge within the safety interval. In addition, the blue curve in Fig. 10 represents the trajectory of state updates under the standard consensus algorithm executed by nodes in the same simulation environment (without considering Sybil attacks). Comparing the trajectory curves of our algorithm and the standard consensus algorithm, it can be seen that the convergence time of the two is almost the same, indicating that the additional costs brought by our algorithm in terms of communication and computation are very small compared with the standard consensus algorithm.

V. Conclusion

In this article, we focused on the study of privacy security and consensus control in the realm of MANs. In particular, we introduced Sybil model and eavesdropper model that consider the characteristics of multiple targets and nondestructive attacks in distributed MANs. Then, WP-PP is proposed, which creatively combines the characteristics of distributed control networks with information security to provide whole-process protection for the privacy of nodes' states. The proposed privacy-preserving mechanism, without needing the cryptographic methods or the assistance of a trusted third party, effectively reduces the computational and communication burden. For the consensus issues, the D-MSR algorithm is designed to remove the impact of Sybil nodes. In addition, sufficient conditions are obtained to determine the network communication topology requirements and the control gain. Extensive simulations were included to illustrate the theoretical results.

References

[1] J. Usevitch and D. Panagou, "Adversarial resilience for sampled-data systems under high-relative-degree safety constraints," *IEEE Trans. Autom. Control*, vol. 68, no. 3, pp. 1537–1552, Mar. 2023.

[2] H. Ishii, Y. Wang, and S. Feng, "An overview on multi-agent consensus under adversarial attacks," *Annu. Rev. Control*, vol. 53, pp. 252–272, Jan. 2022.

[3] F. M. Zegers, M. T. Hale, J. M. Shea, and W. E. Dixon, "Event-triggered formation control and leader tracking with resilience to Byzantine adversaries: A reputation-based approach," *IEEE Trans. Control Netw. Syst.*, vol. 8, no. 3, pp. 1417–1429, Sep. 2021.

[4] W. He, W. Xu, X. Ge, Q.-L. Han, W. Du, and F. Qian, "Secure control of multiagent systems against malicious attacks: A brief survey," *IEEE Trans. Ind. Informat.*, vol. 18, no. 6, pp. 3595–3608, Jun. 2022.

[5] Z. Feng and G. Hu, "Secure cooperative event-triggered control of linear multiagent systems under DoS attacks," *IEEE Trans. Control Syst. Technol.*, vol. 28, no. 3, pp. 741–752, May 2020.

[6] D. Zhang, G. Feng, Y. Shi, and D. Srinivasan, "Physical safety and cyber security analysis of multi-agent systems: A survey of recent advances," *IEEE/CAA J. Autom. Sinica*, vol. 8, no. 2, pp. 319–333, Feb. 2021.

[7] W. Xu, G. Hu, D. W. C. Ho, and Z. Feng, "Distributed secure cooperative control under denial-of-service attacks from multiple adversaries," *IEEE Trans. Cybern.*, vol. 50, no. 8, pp. 3458–3467, Aug. 2020.

[8] D. Zhang, L. Liu, and G. Feng, "Consensus of heterogeneous linear multiagent systems subject to aperiodic sampled-data and DoS attack," *IEEE Trans. Cybern.*, vol. 49, no. 4, pp. 1501–1511, Apr. 2019.

[9] Y. Xu, M. Fang, P. Shi, and Z.-G. Wu, "Event-based secure consensus of mutiagent systems against DoS attacks," *IEEE Trans. Cybern.*, vol. 50, no. 8, pp. 3468–3476, Aug. 2020.

[10] Y. Zhang, Z.-G. Wu, and P. Shi, "Resilient event-/self-triggering leader-following consensus control of multiagent systems against DoS attacks," *IEEE Trans. Ind. Informat.*, vol. 19, no. 4, pp. 5925–5934, Apr. 2023.

[11] W. Xu, D. W. C. Ho, J. Zhong, and B. Chen, "Event/self-triggered control for leader-following consensus over unreliable network with DoS attacks," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 30, no. 10, pp. 3137–3149, Oct. 2019.

[12] H. J. LeBlanc, H. Zhang, X. Koutsoukos, and S. Sundaram, "Resilient asymptotic consensus in robust networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 4, pp. 766–781, Apr. 2013.

[13] W. Fu, J. Qin, Y. Shi, W. X. Zheng, and Y. Kang, "Resilient consensus of discrete-time complex cyber-physical networks under deception attacks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 7, pp. 4868–4877, Jul. 2020.

[14] J. Usevitch and D. Panagou, "Resilient leader-follower consensus to arbitrary reference values in time-varying graphs," *IEEE Trans. Autom. Control*, vol. 65, no. 4, pp. 1755–1762, Apr. 2020.

[15] Y. Wu, X. He, and S. Liu, "Resilient consensus for multi-agent systems with quantized communication," in *Proc. Amer. Control Conf. (ACC)*, Jul. 2016, pp. 5136–5140.

[16] Y. Wang and H. Ishii, "An event-triggered approach to quantized resilient consensus," *Int. J. Robust Nonlinear Control*, vol. 30, no. 11, pp. 4188–4204, 2020.

[17] H. Zhang and S. Sundaram, "Robustness of complex networks with implications for consensus and contagion," in *Proc. IEEE 51st IEEE Conf. Decis. Control (CDC)*, Dec. 2012, pp. 3426–3432.

[18] S. Gil, C. Baykal, and D. Rus, "Resilient multi-agent consensus using Wi-Fi signals," *IEEE Control Syst. Lett.*, vol. 3, no. 1, pp. 126–131, Jan. 2019.

[19] W. Dong and X. Liu, "Robust and secure time-synchronization against Sybil attacks for sensor networks," *IEEE Trans. Ind. Informat.*, vol. 11, no. 6, pp. 1482–1491, Dec. 2015.

[20] V. Renganathan, K. Fathian, S. Safaoui, and T. Summers, "Spoof resilient coordination in distributed and robust robotic networks," *IEEE Trans. Control Syst. Technol.*, vol. 30, no. 2, pp. 803–810, Mar. 2022.

[21] F. Mallmann-Trenn, M. Cavorsi, and S. Gil, "Crowd vetting: Rejecting adversaries via collaboration with application to multirobot flocking," *IEEE Trans. Robot.*, vol. 38, no. 1, pp. 5–24, Feb. 2022.

[22] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 5, pp. 372–383, Oct. 2014.

[23] Y. Shang, "Resilient consensus for expressed and private opinions," *IEEE Trans. Cybern.*, vol. 51, no. 1, pp. 318–331, Jan. 2021.

[24] L. Gao, S. Deng, W. Ren, and C. Hu, "Differentially private consensus with quantized communication," *IEEE Trans. Cybern.*, vol. 51, no. 8, pp. 4075–4088, Aug. 2021.

[25] Z. Huang, S. Mitra, and G. Dullerud, "Differentially private iterative synchronous consensus," in *Proc. ACM Workshop Privacy Electron. Soc.*, Oct. 2012, pp. 81–90.

[26] J. He, L. Cai, and X. Guan, "Differential private noise adding mechanism and its application on consensus algorithm," *IEEE Trans. Signal Process.*, vol. 68, pp. 4069–4082, 2020.

[27] Y. Wang, J. Lam, and H. Lin, "Consensus of linear multivariable discrete-time multiagent systems: Differential privacy perspective," *IEEE Trans. Cybern.*, vol. 52, no. 12, pp. 13915–13926, Dec. 2022.

[28] Q. Li, I. Cascudo, and M. G. Christensen, "Privacy-preserving distributed average consensus based on additive secret sharing," in *Proc. 27th Eur. Signal Process. Conf. (EUSIPCO)*, Sep. 2019, pp. 1–5.

[29] Y. Feng, F. Wang, F. Duan, Z. Liu, and Z. Chen, "Anonymous privacy-preserving consensus via mixed encryption communication," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 8, pp. 3445–3449, Aug. 2022.

[30] M. Ruan, H. Gao, and Y. Wang, "Secure and privacy-preserving consensus," *IEEE Trans. Autom. Control*, vol. 64, no. 10, pp. 4035–4049, Oct. 2019.

[31] C. N. Hadjicostis and A. D. Domínguez-García, "Privacy-preserving distributed averaging via homomorphically encrypted ratio consensus," *IEEE Trans. Autom. Control*, vol. 65, no. 9, pp. 3887–3894, Sep. 2020.

[32] Y. Wang, "Privacy-preserving average consensus via state decomposition," *IEEE Trans. Autom. Control*, vol. 64, no. 11, pp. 4711–4716, Nov. 2019.

[33] D. Fiore and G. Russo, "Resilient consensus for multi-agent systems subject to differential privacy requirements," *Automatica*, vol. 106, pp. 18–26, Aug. 2019.

[34] A. Gusrialdi, "Resilient and privacy-preserving leader-follower consensus in presence of cyber-attacks," *IEEE Control Syst. Lett.*, vol. 7, pp. 3211–3216, 2023.

[35] S. Weng, D. Yue, X. Xie, and C. Dou, "Event-triggered privacy-preserving distributed charging scheduling for plug-in electric vehicle with resilience against denial-of-service attack," *IEEE Trans. Control Netw. Syst.*, early access, May 31, 2024, doi: 10.1109/TCNS.2024.3408008.

[36] Y. Zhang, Z. Peng, G. Wen, J. Wang, and T. Huang, "Privacy preserving-based resilient consensus for multiagent systems via state decomposition," *IEEE Trans. Control Netw. Syst.*, vol. 10, no. 3, pp. 1172–1183, Sep. 2023.

[37] C. Ying, N. Zheng, Y. Wu, M. Xu, and W.-A. Zhang, "Privacy-preserving adaptive resilient consensus for multiagent systems under cyberattacks," *IEEE Trans. Ind. Informat.*, vol. 20, no. 2, pp. 1630–1640, Feb. 2024.

[38] J. Hu, Q. Sun, M. Zhai, and B. Wang, "Privacy-preserving consensus strategy for secondary control in microgrids against multilink false data injection attacks," *IEEE Trans. Ind. Informat.*, vol. 19, no. 10, pp. 10334–10343, Oct. 2023.

[39] Q. Li and M. G. Christensen, "A privacy-preserving asynchronous averaging algorithm based on Shamir's secret sharing," in *Proc. 27th Eur. Signal Process. Conf. (EUSIPCO)*, Sep. 2019, pp. 1–5.
[40] Y. Wu, X. He, S. Liu, and L. Xie, "Consensus of discrete-time multi-agent systems with adversaries and time delays," *Int. J. Gen. Syst.*, vol. 43, nos. 3–4, pp. 402–411, May 2014.
[41] M. Abdelrahim, J. M. Hendrickx, and W. P. M. H. Heemels, "MAX-consensus in open multi-agent systems with gossip interactions," in *Proc. IEEE 56th Annu. Conf. Decis. Control (CDC)*, Dec. 2017, pp. 4753–4758.
[42] D. Deplano, M. Franceschelli, and A. Giua, "Dynamic min and max consensus and size estimation of anonymous multiagent networks," *IEEE Trans. Autom. Control*, vol. 68, no. 1, pp. 202–213, Jan. 2023.
[43] R. Vizuete, C. M. de Galland, P. Frasca, E. Panteley, and J. M. Hendrickx, "Trends and questions in open multi-agent systems," in *Hybrid and Networked Dynamical Systems*. Cham, Switzerland: Springer, 2024, pp. 219–252.
[44] H. J. LeBlanc, H. Zhang, S. Sundaram, and X. Koutsoukos, "Resilient continuous-time consensus in fractional robust networks," in *Proc. Amer. Control Conf.*, Jun. 2013, pp. 1237–1242.
[45] S. M. Dibaji, M. Safi, and H. Ishii, "Resilient distributed averaging," in *Proc. Amer. Control Conf. (ACC)*, 2019, pp. 96–101.
[46] E. Nozari, P. Tallapragada, and J. Cortés, "Differentially private average consensus: Obstructions, trade-offs, and optimal algorithm design," *Automatica*, vol. 81, pp. 221–231, Jul. 2017.
[47] A. Nedic, A. Ozdaglar, and P. A. Parrilo, "Constrained consensus and optimization in multi-agent networks," *IEEE Trans. Autom. Control*, vol. 55, no. 4, pp. 922–938, Apr. 2010.

Yiming Wu received the B.E. degree in automation and the Ph.D. degree in control science and engineering from Zhejiang University of Technology, Hangzhou, China, in 2010 and 2016, respectively.

He held a visiting position from 2012 to 2014 at the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. Since July 2016, he has been with Hangzhou Dianzi University, Hangzhou, where he is currently an Associate Professor with the School of Cyberspace. His main research interests include multiagent networks, security and privacy theory, machine learning, and applications in UAV swarm systems, intelligent transportation systems, and sensor networks.

Chenduo Ying received the B.E. degree in software engineering from NingboTech University, Ningbo, China, in 2020, and the M.S. degree in cyberspace security from Hangzhou Dianzi University, Hangzhou, China, in 2023. He is currently pursuing the Ph.D. degree with the College of Control Science and Engineering, Zhejiang University, Hangzhou.

His main research interests include resilient autonomous unmanned systems, privacy preservation, and distributed system security.

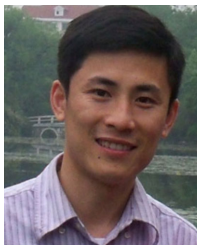
Ning Zheng received the B.S. degree in mathematics form Naval University of Engineering, Wuhan, China, in 1983, and the M.S. degree in computer application from Zhejiang University, Hangzhou, China, in 1990.

He is currently a Full Professor with Hangzhou Dianzi University, Hangzhou. His current research interests include information management system, multiagent system, and information security.

Wen-An Zhang (Senior Member, IEEE) received the B.Eng. degree in automation and the Ph.D. degree in control theory and control engineering from Zhejiang University of Technology, Hangzhou, China, in 2004 and 2010, respectively.

Since 2010, he has been at Zhejiang University of Technology, where he is currently a Professor with the Department of Automation. From 2010 to 2011, he was a Senior Research Associate at the Department of Manufacturing Engineering and Engineering Management, City University of Hong Kong, Hong Kong. His current research interests include networked control systems, multisensor information fusion estimation, and robotics.

Dr. Zhang was a recipient of the Alexander von Humboldt Fellowship from 2011 to 2012. Since September 2016, he has been a Subject Editor for Optimal Control Applications and Methods.



Shanying Zhu (Senior Member, IEEE) received the B.S. degree in information and computing science from the North China University of Water Resources and Electric Power, Zhengzhou, China, in 2006, the M.S. degree in applied mathematics from Huazhong University of Science and Technology, Wuhan, China, in 2008, and the Ph.D. degree in control theory and control engineering from Shanghai Jiao Tong University, Shanghai, China, in 2013.

From 2013 to 2015, he was a Research Fellow at the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, and with Berkeley Education Alliance for Research, Singapore. He joined Shanghai Jiao Tong University in 2015, where he is currently a Full Professor with the Department of Automation. His current research interests include multiagent systems and wireless sensor networks, particularly in coordination control of mobile robots and distributed detection and estimation in sensor networks, and their applications in industrial networks.