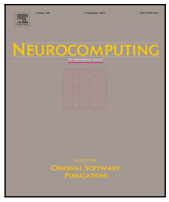
Neurocomputing 597 (2024) 127986

Contents lists available at ScienceDirect

Neurocomputing

journal homepage: www.elsevier.com/locate/neucom



Survey Paper

Differentially private consensus and distributed optimization in multi-agent systems: A review

Yamin Wang [a], Hong Lin [b,*], James Lam [a,c], Ka-Wai Kwok [a]

[a] The Department of Mechanical Engineering, The University of Hong Kong, Hong Kong
[b] The Institute of Intelligence Science and Engineering, Shenzhen Polytechnic University, Shenzhen 518055, China
[c] HKU Shenzhen Institute of Research and Innovation, Shenzhen 518057, China

ARTICLE INFO

Communicated by B. Shen

Keywords:
Consensus
Distributed optimization
Differential privacy
Multi-agent systems

ABSTRACT

In the past few decades, distributed multi-agent system (MAS) control has received growing attention due to its numerous advantages. Nonetheless, the substantial reliance on local information exchange in distributed MAS control has given rise to significant privacy concerns. Differential privacy (DP), a mathematically rigorous privacy notion, has gained popularity as a means of safeguarding privacy across multiple fields, including distributed MAS control. In this paper, we present an in-depth overview of the techniques for preserving DP in distributed MAS control, concentrating on consensus and distributed optimization. We begin by outlining the defining features and modeling of MASs from the control theory perspective. Then, we illustrate the motivation for adopting differentially private mechanisms to protect the privacy of distributed MAS control and present the fundamental principles of DP. Based on them, we investigate the cutting-edge techniques designed to preserve DP in consensus and distributed optimization. This review sheds light on the current landscape of DP applications in distributed MAS control and lays the groundwork for future progress in this essential field.

1. Introduction

The study of multi-agent systems (MASs) has a rich history, with its origins rooted in the exploration of biological phenomena, such as the flocking of birds, the schooling of fishes, and the collaborative hunting of animal herds [1–3]. An MAS is constituted by a collection of autonomous entities, referred to as agents, that can communicate and collaborate over a communication topology [4]. In this way, MASs are able to undertake intricate tasks in a distributed fashion that cannot be effectively performed by a single agent, while simultaneously possessing numerous merits such as low cost, scalability, high fault-tolerance, and robustness [1]. Over the past few decades, the rapid advancement of networking technology has facilitated the integration of distributed MAS control into various applications involving autonomous vehicles, smart grids, and machine learning [5]. Proliferated results have been reported on the distributed control of MASs, most of which are centered on consensus control, formation control, distributed optimization, and distributed estimation. To gain further insights into these recent developments, one may refer to the review papers and the literature therein [6–10].

The distributed nature of MASs offers a multitude of advantages, but it also gives rise to significant privacy concerns. In practice, the deployment of these systems heavily relies on the exchange and aggregation of agents' real-time information, which usually encompasses their privacy-sensitive information, including political opinions, locations, and power consumption [11–13]. Without adequate privacy-preserving mechanisms and secure communication channels, the exchanged information can be intercepted by adversaries or malicious agents for nefarious purposes, such as identity theft, physical harm, or political manipulation, leading to undesirable outcomes. In smart grid systems, for example, smart meters are deployed to constantly collect power consumption data at highly granular levels (minute or second) to achieve specific controlling goals, including economic resource dispatch and fault detection. However, as reported in [14], the information collected by these meters can be exposed to adversaries. By using non-intrusive load monitor methods, adversaries analyze these data and subsequently disclose the privacy of the residents, including details about their daily activities (e.g. home occupancy, sleep patterns, or cooking), health conditions, and the existence and brands of their security appliances. This vulnerability can lead to significant security issues. For instance, a theft armed with this information can determine the optimal time and location for break-ins. In smart transportation systems, traffic flow management necessitates the acquisition of real-time vehicle locations and movements which, however, raises privacy concerns as adversaries can misappropriate and exploit this data to trace individuals' precise

* Corresponding author.
E-mail addresses: yamw@hku.hk (Y. Wang), linhong@szpu.edu.cn (H. Lin), james.lam@hku.hk (J. Lam), kwokkw@hku.hk (K.-W. Kwok).

https://doi.org/10.1016/j.neucom.2024.127986
Received 29 November 2023; Received in revised form 5 March 2024; Accepted 31 May 2024
Available online 5 June 2024

locations [15]. In addition to causing hazardous consequences, these potential privacy violations may lead to a lack of trust among the participating agents, hindering the collaboration and cooperation among agents, which are vital for undertaking the tasks of MASs. Therefore, the privacy concerns arising from MASs must be adequately resolved for their widespread adoption and successful implementation.

In response to the urgent demand for protecting the privacy of distributed MASs, a burgeoning research trend has emerged in recent years, focusing on designing privacy-aware control algorithms for distributed MASs. Various privacy-preserving mechanisms have been considered in this context, such as encryption, anonymization, state decomposition, and differentially private mechanisms. Encryption is a widely embraced technique for protecting static datasets against unauthorized access. However, when it comes to distributed MAS control, encryption is often unfavorable. This is because the implementation of encryption mechanisms usually involves the generation, transmission, and keeping of keys, as well as the decryption of data. These processes are computationally complex and require a substantial amount of resources [16]. Therefore, encryption is ill-suited for distributed MAS control environments, where real-time data are essential for effective control and agents typically operate under constrained computing capabilities and limited resources. As an alternative mechanism, anonymization provides a limited degree of privacy protection by sacrificing total data utility. This proves to be undesirable for distributed MAS control wherein data utility is of paramount importance in accomplishing the intended control objectives. In addition to the aforementioned mechanisms, some works explored state decomposition as an alternative technique. The core principle of state decomposition is to allow only a fraction of information to be shared among agents. Although this approach preserves privacy without compromising data utility, it is difficult to evaluate and guarantee the strength of privacy protection provided.

In recent years, differentially private mechanisms—central focus of this paper—have gained significant popularity in protecting privacy for distributed MAS control due to their rigorous privacy protection, ease of execution, and efficiency in computing. Initially proposed by [17] for static datasets, the concept of differential privacy (DP) distinguishes itself from other privacy-preserving mechanisms by being grounded on a mathematical model that delivers robust and quantifiable privacy protection levels, even in the presence of side information [18]. Moreover, they adopt carefully crafted random noises to perturb the protected target, making their implementation easy and computationally efficient. Owing to these merits, differentially private mechanisms have evolved as the gold standard for ensuring privacy across various fields. They are particularly well suited for preserving the privacy of distributed MAS control, wherein agents are often limited to computational capabilities and resources. A bunch of studies have been conducted on developing distributed MAS control algorithms that integrate differentially private mechanisms to attain desired system performance while ensuring privacy.

In this paper, we narrow our focus on state-of-the-art differentially private distributed MAS control, specifically in the context of consensus and distributed optimization. These two problems allow agents to exchange local information with neighbors and collaboratively make a decision on a shared value based on the received information without relying on a central aggregator, while preserving DP of MASs in terms of initial states, updated states throughout the process, local objective functions, or local constraints. In fact, the consensus and distributed optimization problems are closely correlated. Consensus algorithms provide an essential tool for agents in distributed optimization to process local objective functions in a fully distributed manner and ultimately reach an agreement on the optimal solution. Moreover, the consensus problem can be formulated as a specific form of the distributed optimization problem [19].

One remarkable feature of the algorithms devised for solving the problems of consensus and distributed optimization is the adoption of noise perturbation to guarantee DP, which typically involves Laplacian and Gaussian noises. However, the introduction of random noises may potentially degrade system performance and eventually prevent the agents from reaching the desired solution. Moreover, as reported in many works [20–24], these algorithms usually face a privacy-utility trade-off, where increased noises usually strengthen privacy protection but also compromise convergence accuracy. Therefore, integrating differentially private mechanisms into consensus and distributed optimization is nontrivial and intricate. A critical challenge usually lies in fine-tuning noise injection to balance privacy protection strength and system performance. This delicate balance constitutes a core focus of most studies in this field.

The objective of this paper is to offer an overview of the integration of DP into consensus and distributed optimization in MASs from the perspective of techniques. Despite being in their infancy, these problems hold significant value in the field of distributed MAS control and are worth a summary of the existing theoretical findings. By the end of this paper, the reader will gain an in-depth understanding of the design and implementation of differentially private mechanisms in addressing these challenges. In summary, the main contributions of this paper are threefold:

- *A systematic review of distributed MAS control with DP.* The focused scope of this paper is different from existing works. Despite that some networked systems have been covered in existing surveys, such as cyber–physical systems and power grids, this paper aims to provide a systematic review of recently developed techniques for integrating DP into distributed MAS control. This investigation enables the readers to gain a more up-to-date and in-depth understanding of the latest advancements in this field.
- *A comprehensive literature categorization.* Specifically, the classification of the papers on DP in consensus of MASs is based on types of consensus problems while the classification of the papers on DP in distributed optimization is grounded on types of optimization stepsizes. This wide-reaching taxonomy presents a clear and structured overview of the various methodologies employed in integrating differential privacy in distributed MAS control.
- *Some potential research directions and challenges.* In addition to examining existing research on the application of differential privacy in consensus and distributed optimization, this paper aims to identify potential research directions and challenges in this area. This serves as a roadmap for researchers to further investigate and advance the state-of-the-art in this field.

The notations and abbreviations used in this paper are presented in Tables 1–2. The remainder of this literature survey follows the structure illustrated in Fig. 1. Specifically, Section 2 provides an overview of distributed MAS control and DP. Specifically, it discusses the consensus and distributed optimization in MASs and the privacy issues that arise in this context. Sections 3 and 4 provide an analysis of differentially private techniques that have been proposed for consensus and distributed optimization, respectively. Finally, Section 5 provides a summary of this survey and implications for future research.

2. Distributed multi-agent system control and differential privacy

This section provides an overview of distributed MAS control and DP. We begin by pinpointing the remarkable characteristics of MASs that have a substantial impact on their control performance. Moreover, we introduce the relevant research topics, specifically concerning consensus and distributed optimization. Following this, we inspect the existing or potential mechanisms for protecting privacy in distributed MAS control, which fuels the motivation for adopting DP in distributed MAS control. Lastly, we expose a synopsis of differential privacy in the context of static datasets, including the definitions, fundamental properties, and typical differentially private mechanisms.

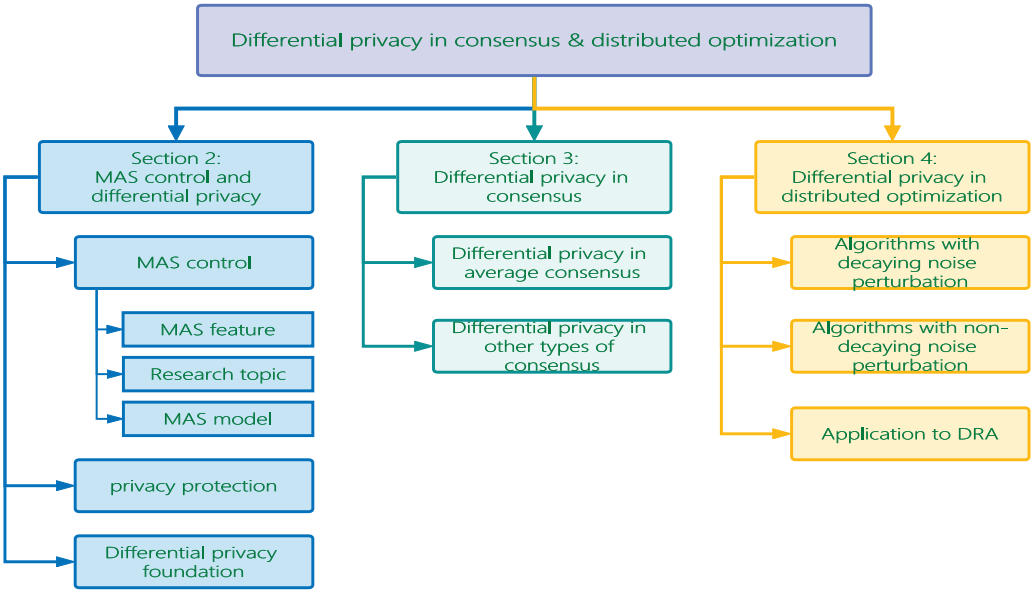


Fig. 1. Structure of this review.

Table 1
List of Abbreviations.

Abbreviation	Referred
MAS	Multi-agent system
IoT	Internet of things
UAV	Unmanned aerial vehicles
DP	Differential privacy
DPC	Differentially private consensus
DO	Distributed optimization
DPDO	Differentially private distributed optimization
i.i.d.	Independent and identically distributed
CDG	Consensus-based distributed (sub)gradient
ADMM	Alternating direction method of multipliers
DRA	Distributed resource allocation

Table 2
List of Notations.

Symbol	Definition
$\mathbb{R}$	Set of real numbers
$\mathbb{R}_{>0}$	Set of positive real numbers
$\mathbb{R}_{\geq 0}$	Set of nonnegative real numbers
$\mathbb{Z}$	Set of integers
$\mathbb{Z}_{>0}$	Set of positive integers
$\mathbb{Z}_{\geq 0}$	Set of nonnegative integers
$\mathbb{R}^n$	Set of n-dimensional vectors
$\mathbb{R}^{n\times m}$	Set of $n\times m$ real matrices
$\mathbb{R}^{n\times m}_{\geq 0}$	Set of $n\times m$ nonnegative matrices
I_n	$n\times n$ identity matrix
1_n	n-dimensional vector with each entry being 1
$\mathbf{0}_{m\times n}$	$m\times n$ zero matrix
$\lvert x\rvert$	Absolute value of the number x
$\lVert x\rVert$	Euclidean norm of the vector x
$\lVert x\rVert_1$	1-norm of the vector x
$\lVert A\rVert$	Induced 2-norm of the matrix A
$[A]_{ij}$	(i,j)-th entry of the matrix A
A^T	Transpose of the matrix A
A^{-1}	Inverse of the matrix A
$\mathrm{diag}\{A_1,\ldots,A_n\}$	Block diagonal matrix with $A_1,\ldots,A_n$ on the diagonal
$A > B$	$A-B$ is positive definite
$A \geq B$	$A-B$ is positive semi-definite
$\mathbb{P}\{\mathcal{S}\}$	Probability of the random event $\mathcal{S}$
$\mathbb{P}\{\mathcal{S}_1 \mid \mathcal{S}_2\}$	Probability of the random event $\mathcal{S}_1$ conditioned on the random event $\mathcal{S}_2$
$\mathrm{Lap}(\mu,b)$	Laplace distribution with mean value μ and variance $2b^2$
$\mathbb{N}(\mu,h^2)$	Normal distribution with mean value μ and variance h^2
$\mathbb{F}_v(\cdot)$	Cumulative function of the random variable v
$\mathbb{E}\{\cdot\}$	Mathematical expectation
$\mathrm{Var}(\cdot)$	Mathematical variance
$\mathcal{R}(\cdot)$	Range space of a function
$f_1\circ f_2(\cdot)$	Composition of function: $f_1(f_2(\cdot))$
$\mathrm{sgn}(\cdot)$	Sign function
$\in$	Belong to

2.1. Distributed multi-agent system control

The advent of the Internet of Things (IoT) has profoundly refashioned conventional end-to-end control systems whose components, including the input and the output, are controlled as an integrated entity. This shift has paved the way for the development of distributed MAS control paradigms and their versatile applications in various fields. In this subsection, we first discuss two essential research topics in the field of distributed MAS control—consensus and distributed optimization, which are the focuses of this paper. Furthermore, we identify the key research considerations and challenges pertinent to these two problems. Subsequently, we introduce the graph theory, which is a vital tool in the theoretical analysis of distributed MAS control, and the mathematical formulation of distributed MAS control.

2.1.1. Features of multi-agent systems

The implementation of distributed MAS control relies on autonomous agents that form a cohesive multi-agent control system and information sharing enabled by their underlying communication topology. This sets the stage for us to characterize MASs by four salient features that significantly impact the challenges and methodologies in distributed MAS control, namely: agent model, information packet, communication graph, and communication strategy.

Agent model: The model of an agent in distributed MAS control is described by a dynamic system, which depends on the underlying assumptions and the cooperative task to be undertaken. Typically, according to the proportionality relationship between input and output, these models can be classified into two categories: linear and nonlinear. The analysis tools for these two classes of MASs are substantially different.

Information packet: Due to practical issues such as restricted bandwidth and environmental interference, MASs often suffer from network congestion, latency, connection failures, communication channel fading, and attacks [25]. These communication imperfections with MASs

could lead to information packets experiencing time delays, packet losses, quantization, and exogenous disturbance [26,27].

Communication graph: In distributed MAS control, the communication graph among agents plays an essential role in determining the overall performance of distributed MASs. The communication graph can be characterized in different ways, such as being undirected or directed and fixed or switching. In an undirected graph, the information stream between agents is bilateral, while the information in a directed graph may only flow in one direction. Moreover, for a static graph, the link between two agents remains consistent over time. Conversely, a switching graph of an MAS permits variations of links as agents join, depart, or relocate within the MAS.

Communication strategy: There are two ways for agents to measure and transmit information to their neighbors. The first approach is the time-triggered strategy, in which agents constantly monitor the environment and deliver the information to their neighbors in predetermined time intervals. This communication strategy is relatively easy to execute but resource-consuming and environmentally demanding. The second approach is the event-triggered strategy, which is proposed to avoid unnecessary resource consumption of communication and computation in the time-triggered strategy. In this strategy, agents initiate the detection of the environment and the subsequent transmission of the measured information to the neighbors only when a specific event condition regarding system dynamics is met. Although the event-triggered strategy is resource-saving, its design and the development of the corresponding control algorithm are complicated due to various restrictions, such as the Zeno phenomenon [28–30].

2.1.2. Research topics

A substantial body of research has focused on developing distributed control algorithms for MAS with remarkable features identified above. These algorithms allow MASs to perform diverse control tasks, among which consensus control, formation control, distributed optimization, and distributed estimation have stood out as prominent investigation topics [31]. In what follows, we review the problems of consensus and distributed optimization, which are the focuses of this paper. A close connection exists between these two problems, as the consensus problem can be regarded as a specific instance of the distributed optimization problem [19]. Moreover, consensus algorithms are instrumental in addressing the distributed optimization problem, enabling agents to compute the optimal solution cooperatively without an aggregator. Regarding other research directions, the reader may refer to the recent survey papers for in-depth insights [32–34].

Consensus of MASs: The consensus problem is regarded as a fundamental research topic in the distributed control of MASs. It has garnered considerable attention due to its versatile applications in multiple fields, including swarm robotics, smart grids, economics, and social networks [35–39]. The objective of the consensus problem is to design a consensus protocol or algorithm that drives agents to agree upon a certain value, referred to as consensus value, through local information exchanged over the underlying communication topology. The consensus value can be any quantity of interest depending on the specific application and the goals of MASs. For instance, in cooperative UAVs, the consensus value may present the desired altitude to attain [40]. In economics, the consensus value may correspond to the common confidence in a particular price [41]; whereas, in social networks, it could be the shared opinion on a political topic that a group of individuals aim to achieve [42]. The theoretical formulation and analysis of the consensus problem can be traced back to the work in [4]. This groundbreaking work pioneered the use of graph theory in the analysis of consensus performance, marking a significant shift from simulation-based approaches to more theoretically grounded analysis. Since then, many scholars have investigated the consensus problem by considering MASs with various features identified previously, such as time delays [43–47], switching communication graphs [48–51], and packet losses [52,53]. These works usually involve evaluating consensus models, designing consensus protocols, and analyzing consensus performance.

Distributed optimization: Apart from the consensus problem, the distributed optimization problem is another critical research focus of MAS control, as it offers a framework for treating many essential tasks in MASs. In power systems, for instance, one can optimally dispatch a set of distributed energy resources by solving a distributed optimization problem that minimizes the total generation cost subject to the demand and the capacity constraints of generators [54]. Another example can be found in machine learning, where distributed optimization algorithms enable training tasks, such as regularized empirical risk minimization [55,56], to be carried out by multiple machines or processors in a fully distributed manner. The aim of the distributed optimization problem is to design a distributed algorithm such that agents update their states in the pursuit of reaching consensus on the optimal solution based on local information, without relying on a central aggregator. The defining feature of distributed optimization is that each agent is only available to its own local objective function and decision variable. A stream of algorithms has been released for distributed optimization from different standpoints. These algorithms can be classified based on the features of MASs and the attributes of the distributed optimization problem, such as the handling of constrained or unconstrained problems, the processing in discrete-time or continuous-time settings, and the adoption of diminishing or fixed step sizes.

2.1.3. Graph theory

In MASs, the interaction relationship between agents can be modeled by a graph. Since the utilization of the Laplacian matrix in the analysis of consensus performance, as presented in the seminal work [4], graph theory has emerged as an indispensable tool for analyzing the system performance of distributed MAS control. This subsection will review some basic terminologies, notations, and basic results concerning graph theory.

Consider a directed graph (digraph) $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{A})$ with N nodes, where $\mathcal{V} = \{1, \dots, N\}$ and $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ are the node set and the edge set, respectively. For all $i \in \mathcal{V}$, node i represents ith agent. An edge in $\mathcal{E}$ is defined as an ordered pair of nodes, represented as (i, j), which indicates that agent j can receive information from agent i. Specifically, a graph is referred to as undirected if $(i, j) \in \mathcal{E}$ implies $(j, i) \in \mathcal{E}$. Node j is an in-neighbor of node i if $(j, i) \in \mathcal{E}$, and the set of all in-neighbors of node i is denoted by $\mathcal{N}_i$. Moreover, $\overline{\mathcal{N}}_i = \{i\} \cup \mathcal{N}_i$. In a digraph, a directed path from node i_1 to node i_2 is an ordered set of edges $\{(i_1, j_1), (j_1, j_2), \dots, (j_{m-1}, j_m), (j_m, i_2)\}$. A digraph $\mathcal{G}$ is strongly connected if there exists a directed path starting from node i to node j for any two distinct nodes $i, j \in \mathcal{V}$. Similarly, an undirected graph is connected if any two distinct nodes can be connected by an undirected path. $\mathcal{A}$ refers to the weighted adjacency matrix of a graph $\mathcal{G}$ with $[\mathcal{A}]_{ij} > 0$, if $(j, i) \in \mathcal{V}$; and $[\mathcal{A}]_{ij} = 0$, otherwise. Thus, the weighted adjacency matrix of an undirected graph is symmetric. Moreover, the weight matrix of a graph $\mathcal{G}$, denoted by W, is row stochastic with each element satisfying $[W]_{ij} > 0$ if $(i, j) \in \mathcal{E}$. Graph $\mathcal{G}$ is balanced if $\sum_{j=1}^{N} [\mathcal{A}]_{ij} = \sum_{j=1}^{N} [\mathcal{A}]_{ji}$, or equivalently, if its corresponding weight matrix W is doubly stochastic. $\mathcal{D} = \mathrm{diag}\{d_1, \dots, d_N\}$ is the in-degree matrix of graph $\mathcal{G}$ with $d_i = \sum_{j=1}^{N} [\mathcal{A}]_{ij}$. In addition, $d_{\max} = \max_{i \in \mathcal{V}} \{d_i\}$ and $d_{\min} = \min_{i \in \mathcal{V}} \{d_i\}$ represent the maximum and the minimum in-degree of $\mathcal{G}$, respectively. L defines the Laplacian matrix of graph $\mathcal{G}$ with $[L]_{ij} = -[\mathcal{A}]_{ij}$, if $i \neq j$; and $[L]_{ii} = \sum_{j=1}^{N} [\mathcal{A}]_{ij}$. It can be readily verified that 1_N is the right eigenvector of L corresponding to the eigenvalue 0. Moreover, 1_N^T is the left eigenvector of L with respect to the eigenvalue 0 when graph $\mathcal{G}$ is balanced, that is, $1_N^T L = L 1_N = 0$.

2.1.4. Multi-agent system model

Consider an N-agent MAS in which agents communicate over a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$. Let $x_i(k) \in \mathbb{R}^n$ and $u_i(k) \in \mathbb{R}^m$ be the state and control input of agent i, respectively. Each agent receives information from the neighbors and updates the dynamics of its state using the collected information in either a time-triggered or event-triggered manner. For simplicity, we present the system model of each agent using a time-triggered strategy:

$$\begin{aligned} &\text{Discrete time:} \\ &x_i(k+1) = f_i(x_i(k), u_i(k)), \quad \forall k \in \mathbb{Z}_{\geq 0}, \forall i \in \mathcal{V}; \\ &\text{Continuous time:} \\ &\dot{x}_i(t) = f_i(x_i(t), u_i(t)), \quad \forall t \in \mathbb{R}_{\geq 0}, \forall i \in \mathcal{V}. \end{aligned} \tag{1}$$

Here, the decision function f_i and the control input u_i are contingent upon the assumptions and the specific problem to be dealt with. For instance, in the consensus problem, one typical discrete-time system model for an agent can be described as: For all $i \in \mathcal{V}$ and for all $k \in \mathbb{Z}_{\geq 0}$:

$$\begin{aligned} x_i(k+1) &= A_i x(k) + B_i u_i(k), \\ u_i(k) &= K_i \sum_{j \in \mathcal{V}} [\mathcal{A}]_{ij} (x_j(k) - x_i(k)), \end{aligned} \tag{2}$$

where A_i, B_i are real-valued system matrices of agent i with compatible dimensions, and K_i is the controller gain matrix of agent i to be designed.

2.2. Privacy protection in distributed multi-agent system control

The distributed architecture of MASs exposes the agents to a high risk of privacy infringements. In the absence of adequate privacy protection and reliable communication channels, adversaries can effortlessly spy on the communication channels and the devices used by the agents, thereby stealing the private information of agents. Protecting privacy in distributed MAS control is a challenging and ongoing assignment that demands careful consideration of multiple factors. This is mainly because the protection of privacy often undermines the performance of systems, and therefore, a balance should be struck between achieving desired system performance and ensuring a sufficient level of privacy protection. Moreover, within the context of distributed MAS control, computational efficiency and resource-saving must be prioritized, given that the majority of agents are relatively simple with limited capabilities of sensing, computing, and communication.

To date, considerable efforts have been devoted to addressing the potential privacy risks in distributed MAS control. One possible idea for addressing this issue is to refine pre-existing privacy-preserving mechanisms, which were initially devised for static datasets, to accommodate the unique features of distributed MAS control. Another viable way is to develop a novel privacy-preserving mechanism based on a theoretical framework covering multiple privacy settings for distributed MAS control. Moving forward, we examine these mechanisms and discuss their advantages and disadvantages in protecting privacy for distributed MAS control. This drives the motivation for adopting DP in distributed MAS control.

Anonymization mechanisms, such as k-anonymity, l-diversity, and t-closeness, have been well established and widely recognized for their effectiveness in protecting the privacy of static datasets [57]. However, these mechanisms may be undesirable for preserving privacy in distributed MAS control due to their significant decline in data utility and insufficient privacy protection. To be precise, anonymization mechanisms usually work by eliminating identifiable information with personal data, resulting in a significant loss of important information. This is unfavorable for distributed MAS control, where the utility of shared information is of paramount importance for collaborative decision-making. Furthermore, anonymization mechanisms are vulnerable to side information under linkage attacks and can only offer limited privacy protection, as evidenced by high-profile incidents, such as the breaches of users' identities and movie preferences in the Netflix prize [58], the re-identification of taxi trips from an anonymized New York City taxi datasets [59], and the re-identification of individuals from anonymized health records [60].

Encryption mechanisms are another solution to safeguarding privacy in static datasets, which effectively prevent unauthorized access by rendering the data unreadable without the corresponding decryption keys. Many scholars have endeavored to combine encryption mechanisms with distributed MAS control, among which homomorphic encryption has emerged as a prevalent method [61–64]. Unfortunately, these encryption mechanisms also have their drawbacks when applied to distributed MAS control. First, the execution of an encryption mechanism typically includes the generation, delivery, and storage of public and private keys, which is computationally burdensome and resource-intensive for agents with limited computational competence or subject to real-time restrictions [65]. Second, in scenarios where communication links between agents are broken or unreliable, such as in mobile ad-hoc networks, key transmission can be problematic, ultimately impeding the implementation of encryption mechanisms.

Apart from the aforementioned techniques, a group of privacy-preserving mechanisms have been devised for distributed MAS control to safeguard privacy, whose key idea is to hide a portion of privacy-sensitive information that is exchanged for computing. These mechanisms include but are not limited to state decomposition [66,67], node decomposition [68], and partial information transmission [69]. Despite their potential to attain accurate convergence, these privacy-preserving mechanisms provide limited privacy protection: the privacy of MASs is only ensured for specific communication topologies and the extent of knowledge adversaries possess about the systems.

In recent years, a notable increase in literature has been witnessed using noise perturbation strategies for privacy preservation in distributed MAS control. In this regard, various privacy notions have been proposed to evaluate the privacy strength of the proposed mechanisms from diverse standpoints, such as observability [70], maximum likelihood estimation [71], indistinguishability [72], and the difference between the estimated data and the original data [73]. Among these privacy notions, DP has stood out since it offers a strong privacy protection strength while guaranteeing satisfactory control performance. The notion of DP was initially proposed in [17] for static datasets. It employs a statistical model to rigorously formulate the privacy guarantee strength. The fundamental idea of differentially private mechanisms is to inject calibrated noises into a dataset such that the processed dataset does not change significantly with slight variations in the original one. In this way, the confidentiality of the processed dataset cannot be compromised even in the worst case where adversaries are accessible to the processed dataset and any side information. The superiorities of differentially private mechanisms over other mechanisms include solid mathematical evaluation of the privacy protection strength, immunity to side information, and lightweight computational overhead, which make them especially attractive to privacy-preserving MAS control. A detailed comparison of the aforementioned privacy-preserving techniques is presented in Table 3, in which the advantages, disadvantages, and applicability in distributed MAS control are thoroughly discussed.

2.3. Foundations of differential privacy

The notion of DP was initially introduced by [17] to protect against privacy breaches of static datasets. In the DP setting, adversaries are unable to distinguish the outputs of two adjacent datasets with great confidence, irrespective of any side information [17]. Therefore, differentially private mechanisms guarantee the non-identifiability of an individual within the protected dataset. Numerous variants of DP have been proposed to meet different privacy protection requirements, including Rényi DP [74] and concentrated DP [75]. In this subsection, we specialize our focus on the basic concept of DP, which was initially proposed by [17]. We begin by introducing the formal definitions of ϵ-DP and (ϵ, δ)-DP, along with their fundamental properties. Subsequently, we present randomized mechanisms that are typically applied to preserve DP of static datasets with numerical query results.

Table 3
Comparison of privacy techniques for distributed multi-agent systems control.

Privacy Technique	Description	Advantages	Disadvantages	Applicability in Distributed MAS Control
Anonymization	Remove personally identifiable information from data	Easy to implement; reduce disclosure risks	Lack data utility; provide weak privacy guarantees (e.g., vulnerable to re-identification attacks)	Inapplicable as data utility is essential for distributed MAS control
Encryption	Generate and assign public and private keys to transmitted data	Preserve original data; restrict unauthorized access	Computationally demanding; do not protect against all privacy threats (e.g., metadata analysis)	Well performed only when agents have sufficient computational ability
Partial Information Concealing	Share only a portion of private data while keeping the rest secret	Preserve data utility; reduce disclosure risks	Provide limited privacy guarantees; effectiveness depends on communication topology and adversaries' knowledge	Applicable for MASs without strong privacy requirements; requires careful control algorithm design
Noise Injection Mechanism	Inject calibrated random noise into data	Less restrictive in implementation than differential privacy; reduce disclosure risks	Reduce data utility; provides weaker privacy guarantees than DP; require careful parameter tuning	Applicable when differential privacy is too restrictive or complex; encounter utility-privacy trade-off
Differential privacy	Inject calibrated random noise into data	Offer rigorous and quantifiable privacy guarantees; prevent individual records from being identified	Reduce data utility; require careful parameter tuning	Promising for sharing aggregate data without revealing individual data points; encounter utility-privacy trade-off

2.3.1. Definitions and basic properties

The core idea of DP is to ensure the indistinguishability of the outputs produced for two adjacent datasets. As such, it is vital to properly define the adjacency relationship, which characterizes how close two datasets are in terms of their contents, for attaining DP. This relationship can be defined over various distance metrics, such as Hamming distance, Manhattan distance, Euclidean distance, Chebyshev distance, and Minkowski distance, depending on the strength of the required privacy protection and the specific content of the dataset being safeguarded [17,76–78].

Prior to introducing the definition of adjacency between two datasets grounded on the Hamming distance, let us first comprehend the underlying implication of this distance metric. The Hamming distance evaluates the dissimilarity between two datasets of equal length by enumerating the number of positions at which the corresponding data differs. With this in mind, we formally introduce the definition of the adjacency relationship between two static datasets, which is originally proposed by [17] based on Hamming distance.

Definition 1 (*Adjacency [17]*). Two datasets $\mathcal{S}_a = \{s_1^a, \dots, s_N^a\}$ and $\mathcal{S}_b = \{s_1^b, \dots, s_N^b\}$ are adjacent, denoted by $\mathrm{Adj}(\mathcal{S}_a, \mathcal{S}_b)$, if the Hamming distance between them is no greater than 1. In other words, these adjacent datasets differ in at most one element.

With the definition of adjacent datasets, we are now ready to introduce the concept of DP.

Definition 2 (*Differential Privacy [17]*). Let $\mathbf{H}$ be a collection of randomized mechanisms that regard a dataset as an input and produce an output. For prescribed $\epsilon \in \mathbb{R}_{>0}$ and $\delta \in [0, 1)$, a randomized mechanism $\mathcal{H} \in \mathbf{H}$ is said to preserve (ϵ, δ)-DP, if for any pair of adjacent datasets $\mathcal{S}_1$ and $\mathcal{S}_2$ and for any $\mathcal{O} \subseteq \mathcal{R}(\mathcal{H})$ the following inequality holds:

$$\mathbb{P}\left\{\mathcal{H}(\mathcal{S}_2) \in \mathcal{O}\right\} \leq e^{\epsilon}\mathbb{P}\left\{\mathcal{H}(\mathcal{S}_1) \in \mathcal{O}\right\} + \delta, \tag{3}$$

where the probability is taken over the coin flips of the randomized mechanism $\mathcal{H}$. When $\delta = 0$, $\mathcal{H}$ is said to be ϵ-differentially private.

In essence, DP ensures the outputs of two neighboring datasets exhibit similar behaviors. In this regard, when the adjacency relationship is depicted in Definition 1, adversaries cannot ascertain the presence or absence of an individual in the private database. This similarity is rigorously quantified through a probabilistic model with a pair of parameters (ϵ, δ), known as the privacy budget. Given a sample ξ drawn from $\mathcal{H}(\mathcal{S}_1)$, let the corresponding privacy loss, represented as $\mathbb{L}_{\mathcal{H}(\mathcal{S}_1)|\mathcal{H}(\mathcal{S}_2)}(\xi) = \log\left(\mathbb{P}\{\mathcal{H}(\mathcal{S}_1) = \xi\}\right) - \log\left(\mathbb{P}\{\mathcal{H}(\mathcal{S}_2) = \xi\}\right)$, be the ratio of observing ξ in both neighboring datasets. Then, (ϵ, δ)-DP states that the absolute value of the privacy loss is constrained by ϵ with a confidence level of no less than $1-\delta$, for any pair of adjacent datasets [17]. As the absolute value of the privacy loss approaches zero, the outputs of the two neighboring datasets are more alike. Therefore, smaller values of ϵ and δ yield stronger privacy guarantees, making ϵ-DP a more rigorous privacy notion than (ϵ, δ)-DP.

Following the definition of DP, we encapsulate its essential features: immunity to post-processing and composition.

Post-processing: One noteworthy property of DP is its post-processing immunity. Specifically, for a (ϵ, δ)-differentially private mechanism $\mathcal{H}$ and any function $\mho$, the composition $\mho \circ \mathcal{H}$ is also (ϵ, δ)-differentially private [17]. In other words, adversaries cannot reduce the privacy of the output produced by a differentially private mechanism through any subsequent computations on it if they have no extra knowledge about the private dataset.

Composition: Composition is another important feature of DP, which enables a conservative calculation of the privacy budget for performing multiple differentially private mechanisms on the same dataset. By leveraging this property, it is possible to ascertain whether a composite mechanism adheres to the DP budget and to allocate the overall privacy budget to each mechanism effectively. The composition property of DP can be characterized as sequential and parallel. Sequential composition works for a composition mechanism that results from the sequential execution of multiple differentially private mechanisms on the same dataset [79]. In this regard, the overall privacy budget is the cumulative sum of individual mechanisms' privacy budgets. Conversely, parallel composition considers a scenario where multiple differentially private mechanisms are applied to disjoint subsets of the same dataset. In this case, the overall privacy budget is the most prominent privacy budget among the individual differentially private mechanisms [79].

2.3.2. Typical mechanisms

When designing a differentially private mechanism, two fundamental issues should be addressed: (1) how to select suitable random noises that are effective in obscuring private data while still allowing for meaningful analysis; (2) how to determine the optimal magnitude of these random noises that balance the privacy budget and data utility. The mainstream way to preserve DP is the noise-adding mechanism, in which calibrated noises are added to the protected dataset. In this subsection, we exhibit two widely-used noise-adding mechanisms for

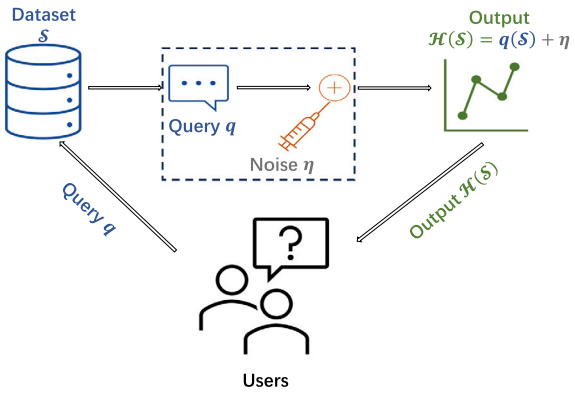


Fig. 2. Diagram of a noise-adding mechanism for preserving DP.

preserving DP of static datasets in the context of numerical query results: Laplace mechanism and Gaussian mechanism.

Noise-Adding Mechanism

$$\mathcal{H}(S) = q(S) + \eta, \tag{4}$$

where $\eta \in \mathbb{R}^N$ is the additive random noise to be designed.

Assume $q(S)$ be a query function of a dataset S that generates real-valued results: $q : S \to \mathbb{R}^N$. Then, the noise-adding mechanism $\mathcal{H}$ can be formalized as presented above.

An illustrative diagram of the noise-adding mechanism $\mathcal{H}$ is presented in Fig. 2.

In DP, the sensitivity of the query function q, denoted as $\boldsymbol{\Delta}(q)$, is to capture the worst-case scenario in terms of how much the outputs of the query function can differ for two adjacent datasets. Mathematically, it can be defined as $\boldsymbol{\Delta}(q) = \max_{\mathrm{Adj}(S_a,S_b)} \|q(S_a) - q(S_b)\|$, where the vector norm typically involves L_1-norm, L_2-norm, and maximum norm [78]. For a prescribed privacy budget, the magnitude of the additive noises in (4) usually depends on the sensitivity of the query function. Essentially, to maintain a desired level of privacy protection, the amount of required additive noises increases as the sensitivity of the query function rises, leading to reduced data utility.

Laplace mechanism: Laplace mechanism was primarily developed in [18] to preserve ϵ-DP of static datasets with numerical query functions. In Laplace mechanism, random noises drawn from Laplace distribution are added to every coordinate of the query function. Given a prescribed privacy budget, the magnitude of Laplacian noises in Laplace mechanism is determined by the sensitivity of the query function. Specifically, as demonstrated in [18], Laplace mechanism is ϵ-differentially private if $\eta \sim \mathrm{Lap}\left(0, \frac{\boldsymbol{\Delta}(q)}{\epsilon}\right)$, where the sensitivity $\boldsymbol{\Delta}(q)$ is defined using L_1-norm.

Gaussian mechanism: Gaussian mechanism is another noise-adding mechanism, which employs Gaussian noises instead of Laplacian noises to offer (ϵ, δ)-DP guarantee for the query functions with numerical outputs. Although Gaussian mechanism ensures a slightly weaker privacy guarantee than Laplace mechanism, it is favored over Laplace mechanism in certain applications, such as in linear dynamic systems. This preference arises from the fact that Gaussian mechanism often streamlines its performance analysis, as a Gaussian random vector remains Gaussian upon linear transformation [74]. In particular, for $\epsilon \in (0, 1)$ and $\delta \in \mathbb{R}_{>0}$, Gaussian mechanism is (ϵ, δ)-differentially private if $\eta \sim \mathbb{N}\left(0, \frac{2\boldsymbol{\Delta}^2(q)\log\left(\frac{1.25}{\delta}\right)}{\epsilon^2}\right)$, where the sensitivity $\boldsymbol{\Delta}(q)$ is defined using L_2-norm [17].

In addition to the aforementioned mechanisms, some other noise-adding mechanisms have been well established, such as Staircase mechanism and Uniform mechanism. Further information can be found in the related works [80,81].

3. Differential privacy in consensus of multi-agent systems

Research has been carried out on integrating various privacy-preserving mechanisms into consensus algorithms to achieve the desired consensus while preserving DP of agents' sensitive information. A common feature shared by most of these mechanisms is the perturbation of transmitted information using additive random noises, such as Laplacian noises and Gaussian noises. However, the randomness introduced by the injected random noises potentially impairs the consensus performance, such as the convergence accuracy and convergence speed. Consequently, a fundamental technical difficulty and persistent motif in these investigations are finding a way to effectively mitigate the impact of random noises on the consensus performance while striking a balance between the consensus performance and the preservation of DP. In this section, we review the existing research on differentially private consensus (DPC) problems, outlining it for different consensus objectives involving average consensus, resilient consensus, second-order consensus, and bipartite consensus. A summary of the works on DPC is shown in Table 4.

3.1. Problem formulation

In this subsection, prior to systematically reviewing the theoretical results pertaining to the DPC problem, we offer an overview of various consensus concepts in the context of stochastic agents' dynamics. Additionally, we introduce the fundamental principles of DP, as they are frequently encountered in the relevant literature. Following this, we present the DPC problem.

Existing DPC problems of MASs are treated in the discrete-time framework. This is primarily attributed to the fact that the discrete-time stochastic process offers a more straightforward and amenable framework for implementing consensus algorithms and analyzing the performance of DP, especially when compared with the continuous-time scenario. As a starting point, consider a general form of discrete-time MASs composed of N agents communicating on a graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$. For each agent $i \in \mathcal{V}$, the state dynamics at each update $k \in \mathbb{Z}_{\geq 0}$ is represented as $x_i(k) \in \mathbb{R}^n$. For the DP preservation of the agents, the state information is perturbed by a randomized mechanism $\mathcal{H} : \mathbb{R}^n \to \mathcal{R}(\mathcal{H})$ with carefully designed random noises $\theta_i(k) \in \mathbb{R}^n$ before transmitting it to neighboring agents:

$$\hat{x}_i(k) = \mathcal{H}(x_i(k)), \ \forall i \in \mathcal{V}, \forall k \in \mathbb{Z}_{\geq 0}. \tag{5}$$

At each update $k \in \mathbb{Z}_{\geq 0}$, agent $i \in \mathcal{V}$ receives the state information from its neighbors (as well as the reference input) and updates its state dynamics as follows [82,83]:

$$x_i(k+1) = f_i\left(\hat{x}_i(k), u_i(k), \theta_i(k), \boldsymbol{\Delta}\mathbf{r}_i(k)\right). \tag{6}$$

Here, the function f_i describes the updating law for agent i; $u_i(k)$ is the control input of agent i to be designed, which can be determined by its current blurred state information and the state information received from its neighbors $\{\hat{x}_j(k)\}_{j\in\bar{\mathcal{V}}_i}$; $\boldsymbol{\Delta}\mathbf{r}_i(k)$ denotes the input of reference signal regarding agent i.

Taking into consideration the randomness of $x_i(k)$ arising from the random noises $\theta_i(k)$, we put forth the following definitions to characterize stochastic convergence behaviors. With these definitions in hand, we then present various types of stochastic consensus for MAS (6), which will be later reviewed in this section.

Definition 3 (*Stochastic Convergence [84]*)**.** Consider a sequence of random variables $\{X(k)\}_{k\in\mathbb{Z}_{\geq 0}}$ and a random variable X defined on a common probability space. Then, the convergence of the random sequence $\{X(k)\}_{k\in\mathbb{Z}_{\geq 0}}$ to X can be characterized as follows:

1. Convergence in distribution: $\{X(k)\}_{k\in\mathbb{Z}_{\geq 0}}$ converges to X in distribution, if $\lim_{k\to+\infty}\mathbb{F}_{X(k)}(x)=\mathbb{F}_X(x)$ for x at which $\mathbb{F}_X(x)$ is continuous;
2. Convergence in probability: $\{X(k)\}_{k\in\mathbb{Z}_{\geq 0}}$ converges to X in probability, if $\lim_{k\to+\infty}\mathbb{P}\{\|X(k)-X\|>\varepsilon\}=0$, $\forall\varepsilon>0$;
3. Convergence in mean square: $\{X(k)\}_{k\in\mathbb{Z}_{\geq 0}}$ converges to X in mean square, if $\lim_{k\to+\infty}\mathbb{E}[\|X(k)-X\|^2]=0$;
4. Convergence almost surely: $\{X(k)\}_{k\in\mathbb{Z}_{\geq 0}}$ converges to X almost surely, if $\mathbb{P}\{\lim_{k\to+\infty}X(k)=X\}=1$.

Among these four classes of stochastic convergence, convergence in mean square and convergence almost surely are particularly relevant to the analysis of stability and system performance, and robust control design for dynamic systems. These two convergence notions both entail convergence in probability, which, in turn, implies convergence in distribution. We proceed to present the concepts of consensus examined in this paper, in which the convergence behaviors refer to stochastic convergence defined previously [85].

Definition 4 (*Consensus of Stochastic MASs*)**.** Consider an MAS with stochastic dynamics as given in (6).

1. Static average consensus [20]: Let $\bar{x}_0=\frac{\sum_{i\in\mathcal{V}}x_i(0)}{N}$ be the averaged initial state. Then, for a prescribed pair of nonnegative values (α,γ), MAS (6) is said to reach static average consensus with (α,γ)-accuracy if there exists a random vector $x_\infty\in\mathbb{R}^n$ such that the following conditions are met:
   - $\mathbb{E}[\|x_\infty\|]<+\infty$;
   - $x_i(k)$ converges to x_∞ as $k\to+\infty$, $\forall i\in\mathcal{V}$;
   - $\mathbb{P}\left\{\|x_\infty-\bar{x}_0\|\leq\alpha\right\}\geq 1-\gamma$.

   In addition, when $\mathbb{E}[x_\infty]=\bar{x}_0$, we call MAS (6) achieves unbiased static average consensus.
2. Dynamic average consensus [86]: MAS (6) is said to achieve dynamic average consensus if for all $i\in\mathcal{V}$ $x_i(k)$ converges to $\bar{\mathbf{r}}(k)$ as $k\to+\infty$, where $\mathbf{r}_i(k)\in\mathbb{R}^n$ is agent i's reference signal and $\bar{\mathbf{r}}(k)=\frac{\sum_{i\in\mathcal{V}}\mathbf{r}_i(k)}{N}\in\mathbb{R}^n$ represents the averaged reference signal.
3. Resilient consensus [83]: Let $\mathcal{F}$ be the set of faulty agents. Then MAS (6) is said to achieve resilient consensus if the following conditions are satisfied:
   - $\min_{j\in\mathcal{V}\backslash\mathcal{F}}\mathbb{E}[x_j(k)]\leq\mathbb{E}[x_i(k)]\leq\max_{j\in\mathcal{V}\backslash\mathcal{F}}\mathbb{E}[x_j(k)]$, $\forall k\in\mathbb{Z}_{\geq 0}$ and $\forall i\in\mathcal{V}\backslash\mathcal{F}$;
   - $\|x_i(k)-x_j(k)\|$ converges to 0 as $k\to+\infty$, $\forall i\neq j$ and $i,j\in\mathcal{V}\backslash\mathcal{F}$.
4. Bipartite consensus [87]: If there exists a random vector $x_\infty\in\mathbb{R}^n$ such that $\mathbb{E}[\|x_\infty\|]<+\infty$ and $x_i(k)$ converges to ψx_∞ as $k\to+\infty$, where $\psi\in\{-1,+1\}$.

Although convergence behaviors of the agents in Definition 4 can be any type of stochastic convergence outlined in Definition 3, the focus of the literature on consensus of stochastic MASs is mainly placed on almost sure convergence and mean-square convergence.

In what follows, we present the definitions of DP that have been extensively considered in the context of consensus of MASs, as referenced in [20,22,82]. The main objective of these definitions is to make sure that adversaries who are accessible to all the information shared in communication channels cannot identify any information about initial states. To begin with, we stack the state dynamics of each agent into a vector, constructed as $x(k)=(x_1^T(k),\dots,x_N^T(k))^T\in\mathbb{R}^{Nn}$. Notice that, in a differentially private problem, the communication channels are commonly assumed to be vulnerable to adversaries. Given this scenario, for a fixed $T\in\mathbb{Z}_{\geq 0}$, we denote the potential information set available to adversaries over time horizon T given the initial state $x(0)$ by $\mathcal{I}_{x(0)}(T)=\{\mathcal{H}(x(k))\}_{k=0}^{T-1}$. DP is formulated on the basis of the adjacency concept, which describes the closeness between two datasets that require privacy protection. In this regard, we present the definition of adjacent initial states.

Definition 5 (σ-*Adjacency*)**.** Given a prescribed nonnegative constant $\sigma\in\mathbb{R}_{\geq 0}$, two initial states $x_a(0)$ and $x_b(0)$ in MAS (6) are said to be σ-adjacent if there exists some $i_0\in\mathcal{V}$ such that $\|x_{ai_0}(0)-x_{bi_0}(0)\|_1\leq\sigma$ and $x_{ai}(0)=x_{bi}(0)$, $\forall i\in\mathcal{V}\backslash\{i_0\}$.

Definition 6 (*Differential Privacy Over Time Horizon* T)**.** Consider a time horizon $T\in\mathbb{Z}_{\geq 0}$ and a pair of parameters $\epsilon\in\mathbb{R}_{>0}$ and $\delta\in[0,1)$. A randomized mechanism $\mathcal{H}$ is said to preserve (ϵ,δ)-DP over time horizon T for MAS (6) if for any two σ-adjacent initial states $x_a(0),x_b(0)\in\mathbb{R}^{Nn}$ in MAS (6) and any set $\mathcal{O}_T\subseteq\mathbb{R}^{Nn\times T}$, the following inequality holds:

$$\mathbb{P}\left\{\mathcal{I}_{x_a(0)}(T)\in\mathcal{O}_T\right\}\leq e^{\epsilon\sigma}\mathbb{P}\left\{\mathcal{I}_{x_b(0)}(T)\in\mathcal{O}_T\right\}+\delta. \tag{7}$$

When $\delta=0$, $\mathcal{H}$ is said to preserve ϵ-DP over time horizon T, a more strict form of DP. Furthermore, if the inequality (7) holds for $T\to+\infty$, the mechanism $\mathcal{H}$ is said to preserve DP for MAS (6) over an infinite time horizon.

We now formalize the DPC problem as follows:

DPC Problem

Develop a consensus algorithm integrated with a randomized mechanism that enables agents to reach the desired consensus performance while ensuring DP of agents' sensitive information.

3.2. Differentially private average consensus

In this subsection, we review the existing literature regarding the differentially private average consensus (DPAC) problem depending on the consensus targets: static average consensus and dynamic average consensus. The aim of static average consensus is to achieve consensus on the average of time-invariant initial states, whereas dynamic average consensus seeks to track the average of time-varying reference signals. This distinction between these two categories underscores the difference in the DP protection targets, highlighting the diversity of approaches and objectives within the DPAC problem field.

3.2.1. Algorithms for static average consensus

The differentially private static average consensus (DPSAC) problem involves devising a distributed consensus algorithm incorporating a randomized mechanism, enabling agents to reach an agreement on the average of the initial states while preserving DP of each agent's initial state.

• *Differentially private static average consensus of first-order multi-agent systems:* The work in [20] initially considered the concept of DP in the average consensus algorithm design by perturbing the shared state information with exponentially time-decaying additive Laplacian noises. They investigated a relatively simple scenario involving discrete-time MASs with *first-order scalar* agents interacting on undirected and connected communication graphs, with or without central servers. The proposed algorithm successfully attains mean-square consensus meanwhile safeguarding DP of the initial states over an infinite time horizon. It is noteworthy that the expected consensus value may deviate from the average initial state and could be influenced by the communication graphs. This issue was further examined by the authors of [82], which established the impossibility of achieving the exact average consensus and ensuring DP simultaneously through rigorous proof. As a result, they developed a novel DPSAC algorithm that relaxes the exact convergence requirement to the almost-sure convergence on an unbiased estimate of the averaged initial state. Specifically, for discrete-time MASs with N first-order scalar agents, at each update $k\in\mathbb{Z}_{\geq 0}$, each

agent $i \in \mathcal{V}$ obscures the state information by additive random noise $\theta_i(k) \in \mathbb{R}$:

$$\hat{x}_i(k) = \mathcal{H}(x_i(k)) = x_i(k) + \theta_i(k), \tag{8}$$

and computes the dynamics according to the following equations [82]:

$$\begin{aligned} x_i(k+1) &= x_i(k) + u_i(k) + s_i\theta_i(k), \\ u_i(k) &= g \sum_{j\in\mathcal{N}_i} [\mathcal{A}]_{ij}(\hat{x}_j(k) - \hat{x}_i(k)), \end{aligned} \tag{9}$$

where $s_i \in (0, 2)$ is the design parameter independently chosen by agent i, which enables agents to autonomously select their preferred privacy strength; $g \in (0, \frac{1}{d_{\max}})$ is the fixed step size to be designed.

For the DPSAC algorithm (8)–(9) on undirected and connected graphs, the authors of [82] showed that both almost-sure convergence on an unbiased estimate of the averaged initial state and ϵ-DP of the initial states over an infinite time horizon can be maintained if the injected random noise of each agent is independently drawn from Laplace distribution with time-vanishing variance, that is $\text{Lap}(0, c_i q_i^k)$, with $c_i \in \mathbb{R}_{>0}, q_i \in (|s_1 - 1|, 1)$, $s_i \in (0, 2)$. Building on this condition, they computed the privacy budget ϵ and the convergence accuracy. They also provided the optimal noise design for a given privacy budget, exhibiting a trade-off between these factors: the consensus accuracy is inversely proportional to the protection strength of DP. As such, increasing the desired protection strength of DP leads to a decrease in algorithm accuracy. Their findings identified the trade-off as stemming from the term $s_i\theta_i(k)$, which is essential for achieving DP but concurrently presents a challenge in attaining accurate static average consensus. This work was further refined by [22], in which the convergence rate is characterized as determined by the diminishing rate of injected noises and the spectral radius of the underlying Laplacian matrix. Along the research framework established [20,22,82], a plethora of studies have been conducted, advancing the proposed DPSAC algorithms in various directions to address more complex and realistic scenarios [81,88–95]. One research direction has focused on enhancing the efficiency of the DPSAC algorithms developed in [20,22,82]. The studies in [90,95] integrated an event-triggered mechanism into the DPSAC algorithm proposed in [82] to boost its computing efficiency. However, the assumption of perfect information transmission, as made in the aforementioned literature, is not applicable to a scenario where information is transmitted through digital signals. To tackle this limitation, the authors of [91] adopted a uniform quantized communication strategy in the DPAC algorithm (9), introducing an additional parameter—an exponentially decaying dynamic factor—to counteract the impact of quantization errors on the average consensus performance. Note that the quantization strategy in [91] is practically restrictive since the introduction of an additional parameter heavily relies on the communication topology and the noise decaying rate. The authors of [88] improved the method of [91] by developing a logarithmic dynamic encoding–decoding (LogDynED) quantization strategy, eliminating the need for an additional parameter and subsequently mitigating the impact of quantization errors on the average consensus performance.

In addition to considering a limited set of time-decaying additive random noises with zero mean, such as Laplacian and Gaussian noises, in the DPSAC algorithms, the studies in [81,94] have delved into the statistical analysis of various random noises that preserve DP of the initial states. To be clear, in [81], a DPSAC algorithm was proposed for first-order scalar MASs on connected and undirected graphs, in which general additive scalar random noises with zero mean and exponentially decaying variance were considered in the randomized mechanism. From the distribution perspective, the statistics of additive scalar random noises were characterized for preserving ϵ-DP and (ϵ, δ)-DP of agents' initial states, respectively. This result was applied to the general scalar random noise design for the proposed DPSAC algorithm. Following it, the case of general digraphs whose weight matrices are not necessarily balanced was investigated in [94], where a push-sum algorithm was introduced to overcome the unbalance of weight matrices.

Recently, the authors of [96] covered the DPSAC problem for first-order scalar MASs with positive agents on balanced and strongly connected digraphs. Observe that the random noises commonly adopted in the DPSAC algorithms are additive and require a zero mean for achieving average consensus. These random noises, however, may inadvertently impair the positivity of agents' dynamics, making them infeasible for the case where agents' dynamics is strictly restricted to the nonnegative region. In response to this issue, the authors of [96] integrated independent and identically distributed (i.i.d.) multiplicative nonnegative Gaussian noises into the shared state information. Unlike most available approaches, the variance of the random noises considered in [96] is constant and bounded, avoiding direct disclosure of agents' trajectories. The proposed algorithm achieves mean-square average consensus with a deduced convergence accuracy while preserving (ϵ, δ)-DP of agents.

• *Differentially private static average consensus of general linear multi-agent systems:* Apart from first-order MASs, some works have been conducted for general linear MASs [92,97]. The work in [97] considered a continuous-time MAS with N heterogeneous general linear agents *on balanced and strongly connected digraphs*. For each agent $i \in \mathcal{V}$, let $y_i(t) \in \mathbb{R}^{p_i}$ be the measurement output of agent i at time t and $\phi_i(t) \in \mathbb{R}^{p_i}$ be the corresponding reference state with the initial condition $\phi_i(0) = y_i(0)$. The agents share the reference state information with the neighbors and update their dynamics according to the following output regulation form of linear continuous-time systems [97]: $\forall t \in \mathbb{R}_{\geq 0}, \forall i \in \mathcal{V}$,

$$\begin{aligned} \dot{x}_i(t) &= A_i x_i(t) + B_i u_i(t), \\ y_i(t) &= C_i x_i(t), \end{aligned} \tag{10}$$

where A_i, B_i, C_i are real-valued matrices with compatible dimensions. To ensure ϵ-DP of reference states and maintain the randomness of the shared reference state information in MAS (10) over time, the authors of [97] devised a discrete-time communication scheme that incorporates a randomized mechanism $\mathcal{H}$ for processing the reference states before transmitting them to the neighbors. In this scheme, at each discrete-time update t_k^-, $\forall k \in \mathbb{Z}_{\geq 0}$, the reference state of agent $i \in \mathcal{V}$ is corrupted with random noise $\theta_i(t_k^-)$, resulting in a modified reference state:

$$\hat{\phi}_i(t_k^-) = \mathcal{H}(\phi_i(t_k^-)) = \phi_i(t_k^-) + \theta_i(t_k^-). \tag{11}$$

Here, different from most of the available approaches that use exponentially decaying noises, additive random noises with invariant covariance were adopted in [97] to maintain the randomness of reference states. To reach output average consensus, the authors of [97] developed a distributed hybrid dynamic feedback controller:

$$\begin{aligned} &u_i(t) = K_{1i}x_i(t) + K_{2i}\phi_i(t), \ \forall t \in \mathbb{R}_{\geq 0}; \\ &\dot{\phi}_i(t) = 0, \ \forall t \in (t_k, t_{k+1}), \forall k \in \mathbb{Z}_{>0}; \\ &\phi_i(t_k) = \phi_i(t_k^-) + g(k-1) \sum_{j\in\mathcal{N}_i} (\hat{\phi}_j(t_k^-) - \phi_i(t_k^-)), \ \forall k \in \mathbb{Z}_{>0}, \end{aligned} \tag{12}$$

where K_{1i}, K_{2i} are the controller gain matrices to be designed based on the stochastic approximation method; $g(k) \in \mathbb{R}_{>0}$ is the time-varying controller parameter to be designed.

As demonstrated in [97], MAS (10) on balanced and strongly connected digraphs with the randomized mechanism (11) and the distributed hybrid controller (12) reaches mean-square output consensus on an unbiased estimate of the averaged initial state while preserving ϵ-DP over a finite time horizon. This was accomplished by appropriately designing $\{\theta_i(t_k^-)\}_{k\in\mathbb{Z}_{\geq 0}, i\in\mathcal{V}}$, $\{K_{1i}\}_{i\in\mathcal{V}}$, $\{K_{2i}\}_{i\in\mathcal{V}}$, and $\{g(k)\}_{k\in\mathbb{Z}_{\geq 0}}$, by virtue of the stochastic approximation method. Here, the positive sequence $g(k)$ is non-summable but square summable. In this context, furthermore, the design criteria were provided in [97] for the time-decaying step size $g(k)$ to attain a prescribed consensus accuracy and to

ensure a desired ϵ-DP over an infinite time horizon, respectively. These criteria involve designing $g(k)$ in a specific form and selecting appropriate constants to meet the desired performance and privacy budget, which reveals a trade-off analogous to the scalar case investigated in [22,82].

In addition, the discrete-time case has been addressed in [92] for the DPSAC problem of general linear heterogeneous MASs on balanced and strongly connected digraphs. For all $i \in \mathcal{V}$ and for all $k \in \mathbb{Z}_{\geq 0}$, the following equations hold:

$$\begin{aligned} x_i(k+1) &= A_i x_i(k) + B_i u_i(k), \\ y_i(k) &= C_i x_i(k), \end{aligned} \tag{13}$$

with A_i, B_i, C_i being real-valued matrices equipped with compatible dimensions. Notice that Gaussian noises are prevalent in practice, and their thinner distribution tails contribute to an improved consensus accuracy performance compared to Laplacian noises with identical standard deviation. The authors of [92] adopted exponentially decaying additive Gaussian noises $\theta_i(k)$ to randomize the shared reference state $\phi_i(k)$. A novel DP notion, called ϵ-concentrated DP, was introduced, offering a more precise analysis of the DP budget compared to (ϵ, δ)-DP. Following an approach similar to the study in [97], a discrete-time version of the dynamic feedback controller (12) was proposed, and the corresponding parameters were designed. Under the established results, MAS (13) on balanced and strongly connected digraphs achieves output unbiased average consensus with a convergence rate and preserves ϵ-concentrated DP simultaneously. Moreover, an intriguing result was found that increasing the coupling of each agent dynamics in the communication graph can enhance privacy protection against adversaries.

3.2.2. Algorithms for dynamic average consensus

In contrast to the well-explored static average consensus issue, the dynamic average consensus problem seeks to design a consensus algorithm that drives the agents to track the average of locally available *time-varying* reference signals. The applications of this problem have permeated various research fields, encompassing distributed formation control, distributed state estimation, distributed resource allocation, and distributed unconstrained convex optimization [98]. It is important to note that the dynamic average consensus problem, unlike the static problem which aims at protecting time-invariant initial states, deals with time-varying reference signals as privacy-sensitive information. Although the randomized mechanisms proposed in the available DPSAC algorithms can be applied to the differentially private dynamic average consensus (DPDAC) problem, two nontrivial issues remain unresolved: (1) Can the ϵ-DP of reference signals be maintained, as agents track time-varying reference signals? (2) Is there a trade-off between dynamic average consensus and DP? Alternatively, is it possible to achieve the exact consensus for the DPDAC problem?

In response to these issues, the authors of [86] carried out a study and yielded an intriguing conclusion deviating from the one made in the DPSAC problem: both exact dynamic average consensus and ϵ-DP can be guaranteed when the variations of reference signals gradually decay with time. To safeguard ϵ-differential privacy of the time-varying reference signals, the author of [86] proposed a novel DP concept. This concept establishes an adjacency relationship between two dynamic average consensus problems based on time-varying reference signals by requiring similar steady states of reference signals and imposing a restriction on the change magnitude. Specifically, there exist some $i_0 \in \mathcal{V}$ and positive constant $\tilde{c} \in \mathbb{R}_{>0}$ such that $\|\mathbf{r}_{ai_0}(k) - \mathbf{r}_{bi_0}(k)\|_1 \leq \tilde{c} g_1(k)\beta(k)$ and $\mathbf{r}_{ai}(k) = \mathbf{r}_{bi}(k)$, $\forall i \in \mathcal{V}\backslash\{i_0\}$, hold for all $k \in \mathbb{Z}_{\geq 0}$. Here $\{\mathbf{r}_{ai}(k)\}_{i\in\mathcal{V},k\in\mathbb{Z}_{\geq 0}}$ and $\{\mathbf{r}_{bi}(k)\}_{i\in\mathcal{V},k\in\mathbb{Z}_{\geq 0}}$ are the reference signals corresponding to two different dynamic average consensus problems; $g_1(k) \in \mathbb{R}_{\geq 0}$ and $\beta(k) \in \mathbb{R}_{\geq 0}$ are nonnegative parameters to be designed. They proposed a novel DPDAC algorithm for discrete-time first-order MASs on undirected and connected graphs: $\forall k \in \mathbb{Z}_{\geq 0}, \forall i \in \mathcal{V}$,

$$\begin{aligned} x_i(k+1) &= (1 - g_1(k))x_i(k) + \Delta\mathbf{r}_i(k) + u_i(k), \\ \Delta\mathbf{r}_i(k) &= \mathbf{r}_i(k+1) - (1 - g_1(k))\mathbf{r}_i(k), \\ u_i(k) &= g_2(k) \sum_{j\in\mathcal{N}_i} [A]_{ij}(\hat{x}_j(k) - x_i(k)), \\ \hat{x}_j(k) &= \mathcal{H}(x_j(k)) = x_j(k) + \theta_j(k) \end{aligned} \tag{14}$$

In this formulation, the term $\Delta\mathbf{r}_i(k)$ represents the input of agent i's reference signal, which must decay gradually over time to guarantee convergence to the exact average reference signal. The design parameter $g_1(k) \in \mathbb{R}_{\geq 0}$ is responsible for tuning the input of these reference signals. The time-varying step size $g_2(k) \in \mathbb{R}_{\geq 0}$ plays a crucial role in mitigating the influence of injected noise on consensus performance. Additionally, each element of $\theta_i(k)$, $\forall i \in \mathcal{V}, \forall k \in \mathbb{Z}_{\geq 0}$, is i.i.d.

By virtue of the stochastic approximation method, the study in [86] demonstrated that the DPDAC algorithm (14) is able to reach dynamic average consensus almost surely while preserving ϵ-DP of reference signals over a finite time horizon if random noise $\theta_i(k)$, the design parameters $g_1(k), g_2(k)$, and reference signal $\mathbf{r}_i(k)$ meet certain conditions. Moreover, when the term $\sum_{k=0}^{+\infty} \frac{\sqrt{2}\beta(k)}{\nu_i(k)} < +\infty$, ϵ-DP of reference signals can be preserved over an infinite time horizon, where $\nu_i(k)$ is the standard deviation of $\theta_i(k)$.

3.3. Differential privacy in other types of consensus

In addition to average consensus, some works have integrated differentially private mechanisms into various other consensus problems, including resilient consensus, bipartite consensus, and maximum consensus.

• *Differentially private resilient consensus:* The authors of [83] tackled the differentially private resilient consensus problem for first-order scalar MASs on digraphs. They focused on a scenario where nonfaulty agents seek to achieve consensus while contending with faulty agents who deviate from the standard updating laws of non-faulty agents. To do so, they devised a novel algorithm that modifies the conventional mean-subsequence-reduced algorithm by applying the randomized mechanism (8) to the shared state information. By adhering to the definitions of ϵ-DP and consensus accuracy established in [22,82], both mean-square resilient consensus and ϵ-DP were analyzed. The algorithm proposed in [83] was shown to attain mean-square consensus for non-faulty agents with a certain consensus accuracy when the communication digraph is sufficiently robust. Furthermore, the privacy budget ϵ was characterized in terms of two specific cases: (1) the absence of faulty agents; (2) the presence of faulty agents.

• *Differentially private consensus of high-order multi-agent systems:* Some efforts have also been devoted to dealing with the DPC problem for discrete-time high-order MASs [99,100]. Specifically, in [100], the DPC problem was considered for general linear multivariable MASs on undirected graphs, in which general multivariate random noises are added to the state information before it is sent to the neighbors with the goal of preserving DP of the agents' states at every single iteration. The work in [99] addressed this issue in a scenario where the agents share quantized information over undirected and connected graphs, and their velocities are unmeasurable. In this setting, for each agent $i \in \mathcal{V}$ and for all $k \in \mathbb{Z}_{\geq 0}$, state vector $x_i(k)$ is a two-dimensional vector represented as $(x_{i1}(k), x_{i2}(k))^T \in \mathbb{R}^2$, and $y_i(k) = x_{i1}(k) \in \mathbb{R}$ defines the corresponding measurable output of agent i. Here, $x_{i1}(k) \in \mathbb{R}$ and $x_{i2}(k) \in \mathbb{R}$ represent the position and the velocity of agent i at kth update, $\forall k \in \mathbb{Z}_{\geq 0}$, respectively. To preserve ϵ-DP of the initial states, a randomized mechanism similar to that of [20] was applied to $y_i(k)$ such that

$$\hat{y}_i(k) = \mathcal{H}(y_i(k)) = y_i(k) + \theta_i(k) \tag{15}$$

with $\theta_i(k)$, $\forall i \in \mathcal{V}$, i.i.d. drawn from Lap$(0, c_i q_i^k)$, where $q_i \in (1-s_i, 1)$ is a constant. By adapting the dynamic encoding–decoding (DynED) quantization scheme from [101], a DPC algorithm was proposed in [99]:

$$\begin{aligned}\begin{bmatrix} x_{i_1}(k+1) \\ x_{i_2}(k+1) \end{bmatrix} &= \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x_{i_1}(k) \\ x_{i_2}(k) \end{bmatrix} + \begin{bmatrix} s_i\theta_i(k) \\ u_i(k) \end{bmatrix}, \\ u_i(k) &= g_1 \sum_{j\in\mathcal{N}_i} [\mathcal{A}]_{ij}(\tilde{y}_j(k) - \tilde{y}_i(k)) \\ &\quad + g_2 \sum_{j\in\mathcal{N}_i} [\mathcal{A}]_{ij}(\tilde{x}_{j2}(k) - \tilde{x}_{i2}(k)), \\ &\quad \forall i \in \mathcal{V}, \forall k \in \mathbb{Z}_{\geq 0},\end{aligned} \tag{16}$$

where $s_i \in (0, 1)$ is the privacy parameter; $g_1, g_2 \in \mathbb{R}_{>0}$ are the designing controller parameters; $\tilde{y}_i(k) \in \mathbb{R}$ and $\tilde{x}_{i2}(k) \in \mathbb{R}$ are the estimated value of $\hat{y}_i(k)$ and the estimated value of $x_{i2}(k)$ obtained by the decoder in [101], respectively.

For the consensus algorithm (16) with the randomized mechanism (15), a sufficient condition was established in [99] for reaching mean-square consensus. It should be noted that both the selection of $\theta_i(k)$ and the design of the scaling function for the proposed quantizer in [101] are intricate tasks. Notably, $\theta_i(k)$ must be appropriately generated to avoid quantizer saturation. Furthermore, the scaling function should decay slower than that of $\theta_i(k)$ for the achievement of consensus. The work also revealed that the averaged initial velocity states significantly impact the consensus value of the position states. More precisely, the consensus value of the position states is an unbiased estimate of the averaged initial position state if the averaged initial velocity state is zero. Conversely, the consensus value of the position states will tend toward infinity as time progresses if the averaged initial velocity state is nonzero. Furthermore, an analysis of ϵ-differential budget was conducted, with the accuracy being determined based on a modification of Definition 4, where $\bar{x}_0$ is replaced with $\bar{x}(k)$. The derived results were found to be similar to those in [22,82].

• *Differentially private bipartite consensus:* The aforementioned studies concerning the DPC problem mainly focus on the case of the cooperative relationship between the agents. However, in practical scenarios, the concurrent presence of cooperative and competitive interactions between them is also prevalent in practice [102]. This observation led to the works in [103,104], which formulated the cooperative–competitive interactions between agents within a signed graph. They investigated the bipartite consensus problem of first-order scalar MASs subject to DP:

$$\begin{aligned} x_i(k+1) &= x_i(k) + u_i(k) \\ u_i(k) &= g(k) \sum_{j\in\mathcal{N}_i} [\mathcal{A}]_{ij} \left(\hat{x}_j(k) - \operatorname{sgn}\left([\mathcal{A}]_{ij}\right) x_i(k)\right), \end{aligned} \tag{17}$$

where the step size $g(k) \in \left(0, \frac{1}{d_{\max}}\right)$ can be time-varying. For MAS (17), the authors of [103] considered the fixed step size $g(k) = g$ and devised a novel randomized mechanism tailored to the cooperative–competitive relationship between agents. The proposed mechanism specifically targets the state information transmitted to competitive neighbors by injecting decaying Laplacian noises. In particular, for (17),

$$\hat{x}_j(k) = \mathcal{H}(x_j(k)) = x_j(k) + \frac{1 - \operatorname{sgn}\left([\mathcal{A}]_{ij}\right)}{2}\theta_j(k), \ \forall j \in \mathcal{V}, \tag{18}$$

with $\theta_j(k)$, $\forall j \in \mathcal{V}$, i.i.d. drawn from Lap$(0, c_j q_j^k)$, where $q_j \in (0, 1)$. They demonstrated that when the interaction signed graph is structurally balanced and has a spanning tree, MAS (17) with the randomized mechanism (18) can attain unbiased mean-square bipartite consensus with a specific convergence accuracy and simultaneously preserve ϵ-DP of the initial states against the competitive agents.

Improved upon the work in [103], the authors of [104] relaxed the constraint on the injected noises, allowing for their variances that are not only decaying or constant but also increasing. They considered the following randomized mechanism which injects random noises to the state information transmitted to the neighbors, irrespective of the interaction relationship:

$$\hat{x}_i(k) = \mathcal{H}(x_i(k)) = x_i(k) + \theta_i(k), \ \forall i \in \mathcal{V}, \tag{19}$$

with $\theta_i(k)$ i.i.d. drawn from Lap$(0, q(k))$, where $\{q(k)\}_{k\in\mathbb{Z}_{\geq 0}}$ is a non-negative sequence. By employing the stochastic approximation method, sufficient conditions were established respectively for unbiased mean-square bipartite consensus and for unbiased almost-sure consensus when the communication signed graph is structurally balanced and connected. With the established conditions and drawing upon the research line in [97], the authors characterized the convergence rate in both the mean-square and almost-sure senses for certain forms of $g(k)$ and $q(k)$. Additionally, they provided a design guideline on designing the random noises and the step size to achieve the prescribed privacy budget ϵ over an infinite time horizon, unveiling a trade-off between the consensus performance and the privacy budget in accordance with the existing works. Pursuing this direction, the author in [105] investigated the case of MASs with general linear agents. A novel differential privacy mechanism was established, composed of a classifier and noise injectors applied to both the input and output.

4. Differential privacy in distributed optimization

To date, a multitude of works have focused on developing algorithms to tackle the DO problem within a fully distributed framework while safeguarding DP, specifically in a scenario where global constraints are absent.

Among these studies, the consensus theory established in previously examined DPC problems lays a solid foundation for analyzing the convergence and optimality accuracy. It is essential, however, to note that the design of DP mechanisms for the DPDO problem differs from the DPC problem due to their different privacy protection goals. To be precise, the DPC problem usually addresses privacy-sensitive information related to the shared messages in the algorithm, such as agents' initial states and states evolving over time. In contrast, the DPDO problem may focus on private information pertaining to the shared messages, including agents' states, agents' internal updating variables, such as local objective functions, or local constraints. As such, the noise perturbation strategies for preserving desired DP in the DPDO problem may not be limited to those employed in the DPC problem and can be grouped under two categories: (1) *message perturbation*: adding random noises to shared messages, such as states and (sub)gradients; (2) *objective perturbation*: incorporating random noises into objective functions without altering shared messages. A majority of these algorithms rely on *non-amplifying* random noises, which, however, face a common privacy-utility trade-off similar to DPC algorithms: the simultaneous achievement of accurate optimality and DP remains an arduous endeavor. This primarily stems from the fact that the increased magnitude of perturbation noises ensures stronger DP while also resulting in a rising optimality error, particularly in the absence of parameters that temper the impact of noises on optimization accuracy. Recent work in [106] has applied additive non-decaying random noises to perturb shared messages and proposed a novel DO algorithm to achieve accurate optimality in the almost sure sense while preserving DP.

In this section, we begin by formulating the differentially private distributed optimization problem. Following it, we review the existing DPDO algorithms that adopt diminishing noise perturbation. Subsequently, we introduce a recent study that explored the employment of amplifying noise perturbation as a means of preserving DP. Lastly, we review the application of the DPDO algorithms to the distributed resource allocation problem. A summary of the works on DPDO is presented in Table 5.

Table 4
Summary of differential privacy in consensus of MASs.

Type of consensus	Ref No.	Privacy scenario				MAS feature				
		Private information	Observation available	Privacy criterion	Noise adopted	Agent model	Communication strategy	Topology	Information packet	Consensus performance
Static average consensus	[20]	initial states	infinite time horizon	ϵ-DP	exponentially dec additive Laplacia	first-order	discrete-time	undirected connected	N/A	biased static average consensus in mean square
	[82]	initial states	infinite time horizon	ϵ-DP	exponentially dec additive Laplacia	first-order	discrete-time	undirected connected	N/A	unbiased static average consensus almost surely
	[22]	initial states	infinite time horizon	ϵ-DP	exponentially dec additive Laplacia	first-order	discrete-time	undirected connected	N/A	unbiased static average consensus almost surely
	[90]	initial states	infinite time horizon	ϵ-DP	exponentially dec additive Laplacia	first-order	event-triggered	undirected connected	N/A	unbiased static average consensus in mean square
	[95]	initial states	infinite time horizon	ϵ-DP	exponentially dec additive Laplacia	first-order	event-triggered	undirected connected	N/A	biased static average consensus in mean square
	[91]	initial states	infinite time horizon	ϵ-DP	exponentially dec additive Laplacia	first-order	discrete-time	undirected connected	uniform quantization	unbiased static average consensus in mean square
	[89]	initial states	infinite time horizon	ϵ-DP	additive functiona Laplacian noise w exponentially dec variance	first-order	discrete-time	undirected connected	N/A	unbiased static average consensus in mean square
	[81]	initial states	infinite time horizon	ϵ-DP & (ϵ, δ)-DP	general exponenti decaying additive	first-order	discrete-time	undirected connected	N/A	N/A
	[97]	initial states	infinite time horizon	ϵ-DP	non-decaying Laplacian noise	heterogeneous general linear	hybrid	directed, strongly connected, weight-balanced	N/A	unbiased average output static consensus in mean square
	[94]	states	single iteration	ϵ-DP	general exponenti decaying additive	first-order	discrete-time	directed, strongly connected, weight-unbalanced	N/A	accurate static average consensus in mean square
	[92]	initial states	infinite time horizon	ϵ-concentrate DP	exponentially dec additive Gaussian	heterogeneous general linear	discrete-time	directed, strongly connected, weight-balanced	N/A	unbiased static average output static consensus in mean square
	[88]	initial states	infinite time horizon	ϵ-DP	exponentially dec additive Laplacia	first-order	discrete-time	undirected connected	DynED quantization	unbiased static average consensus almost surely
	[96]	initial states	finite time horizon	(ϵ, δ)-DP	non-decaying mu truncated Gaussia	first-order, positive	discrete-time	directed, strongly connected, weight-unbalanced	N/A	biased static average consensus in mean square
Dynamic average consensus	[86]	reference signal	infinite time horizon	ϵ-DP	Laplacian noise w increasing varian	first-order	discrete-time	undirected connected	N/A	accurate dynamic average consensus almost surely
Resilient consensus	[83]	initial states	infinite time horizon	ϵ-DP	exponentially dec Laplacian noise	first-order	discrete-time	r-robust directed	N/A	resilient consensus in mean square
Bipartite consensus	[103]	initial states	infinite time horizon	ϵ-DP	exponentially dec Laplacian noise	first-order	discrete-time	signed directed, spanning tree, structurally balanced	N/A	bipartite consensus in mean square
	[104]	initial states	infinite time horizon	ϵ-DP	Laplacian noise with varying vari (increasing, const decaying)	first-order	discrete-time	signed undirected, connected, structurally balanced	N/A	bipartite consensus in mean square and almost surely
Second-order consensus	[99]	initial states	infinite time horizon	ϵ-DP	exponentially dec Laplacian noise	second-order	discrete-time	undirected connected	DynED quantization	consensus in mean square

Table 5
Summary of differential privacy in distributed optimization.

Step sizes	Approach	Problem	Ref No.	Privacy scenario		Perturbation strategy	Laplacian Noise adopted	Objective function	Constraint	Topology & delay	Convergence Performance		
				Private information	Observation available						convergence rate	Steady-state error	Trade-off
diminishing, summable	projected CDG	general DO	[107]	objective functions	an infinite number of iterations	state perturbation	exponentially decaying	strongly convex with bounded subgradients	common compact and convex constraint	time-varying directed, strongly connected, weight-balanced	sub-linear	✔	✔
	push-sum based CDG		[108]	initial states and objective functions	an infinite number of iterations	state perturbation	exponentially decaying	strongly convex with bounded subgradients	unconstrained	time-varying strongly connected, weight-unbalanced, column stochastic	sub-linear	✔	✔
diminishing, non-summable	general DO algorithms		[109]	objective functions	an infinite number of iterations	objective perturbation	functional	convex, twice-differentiable, square-integrable	common compact convex constraint	directed	asymptotical	✗	✔
	push-pull based gradient tracking CDG		[106]	objective functions	an infinite number of iterations	state perturbation	amplifying	convex and smooth	unconstrained	directed, weight-unbalanced, column stochastic with spanning tree	sublinear	✗	✗
diminishing	weight-balancing based CDG	online DO	[110]	objective functions	single iteration	state perturbation	decaying	(strongly) convex with bounded subgradients	unconstrained	time-varying directed, strongly connected, weight-unbalanced with known out-degree	sub-linear regrets	✔	✔
	combination of projected CDG with subgradient rescaling		[111]	objective functions	single iteration / a finite number of iterations	state perturbation	decaying	strongly convex with bounded subgradients / generally convex with bounded subgradients	common compact and convex constraint	directed, strongly connected, weight-unbalanced, row stochastic	sub-linear regrets	✔	✔
	push-sum based CDG		[112]	objective functions	single iteration	state perturbation	decaying	strongly convex with bounded subgradients / generally convex with bounded subgradients	unconstrained	jointly strongly connected directed, weight-unbalanced, column stochastic & uniformly bounded delays	sub-linear regrets	✔	✔
constant	combination of distributed inexact gradient and gradient tracking	general DO	[113] [114]	objective functions	an infinite number of iterations	state and gradient perturbation	exponentially decaying	(strongly) convex, smooth	unconstrained	undirected connected	linear	✗	✔
	push-pull based CDG		[24]	objective functions	a finite number of iterations	combination of direction decomposition and gradient perturbation	constant variance	strongly convex with bounded gradients	unconstrained	directed, weight-unbalanced, column stochastic, has a spanning tree	linear	✔	✔
constant	ADMM	ERM	[115]	objective functions	single iteration	dual perturbation/ primal perturbation	Laplacian noise/ functional	strongly convex and doubly differentiable with bounded gradients and Hessian matrix	unconstrained	undirected connected	linear	✗	✔
	modified ADMM		[116]		a finite number of iterations	dual perturbation	functional						
	modified recycled ADMM		[117]		a finite number of iterations	dual perturbation	functional						
diminishing, non-summable	inexact alternating minimization algorithm	DRA	[118] [119]	objective functions and constraints	a finite number of iterations	dual state perturbation	exponentially decaying	strongly convex, smooth	convex local constraints	undirected, connected	sublinear	✔	✔
constant	combination of distributed inexact gradient with gradient tracking		[120] [121]	objective functions	an infinite number of iterations	dual state and gradient perturbation	exponentially decaying	strongly convex, smooth	convex local constraints	undirected, connected	linear	✗	✔
	push-pull based gradient tracking CDG		[122]	objective functions	single iteration	combination of dual gradient perturbation with gradient-tracker decomposition	constant variance	strongly convex, smooth	box local constraints	directed, strongly connected, weight-unbalanced, column stochastic	linear	✗	✔
	combination of state predictor with gradient tracking		[123]	initial states	an infinite number of iterations	dual gradient perturbation	exponentially decaying	strongly convex, twice differentiable	box local constraints	undirected, connected & heterogeneous delays	linear	✗	✔

4.1. Problem formulation

This subsection lays the groundwork for systematically reviewing the relevant works on differentially private distributed optimization. First, we introduce a general form of the DO problem to provide a foundation for understanding the problem domain. Next, within the context of the DO problem, we present the commonly considered definitions of DP, which serve as the basis for developing privacy-preserving algorithms. Finally, we formulate the DO problem subject to DP.

DO Problem

Design a fully distributed algorithm that solves the following optimization problem (20) without the need for a central aggregator:

$$\begin{aligned} &\min_{x\in\mathbb{R}^{Nn}} \sum_{i\in\mathcal{V}} F_i(x_i) \\ &\text{s.t. } x_i = x_j,\ \forall i,j\in\mathcal{V}; \\ &\quad x_i\in\Omega_i,\ \forall i\in\mathcal{V}. \end{aligned} \tag{20}$$

To begin with, consider an MAS consisting of N agents who communicate through a graph $\mathcal{G}=(\mathcal{V},\mathcal{E},\mathcal{A})$. Each agent $i\in\mathcal{V}$ is equipped with a local convex objective function $F_i:\mathbb{R}^n\to\mathbb{R}$ that is exclusively known to the respective agent. The set of local objective functions is be denoted as $\mathbf{F}=\{F_i:\mathbb{R}^n\to\mathbb{R},\forall i\in\mathcal{V}\}$. Let $\mathbf{\Omega}=\cap_{i\in\mathcal{V}}\Omega_i\subseteq\mathbb{R}^n$ be the domain of optimization, respectively. We can then define the above DO Problem $\mathcal{P}$ specified by a tuple of parameters $(\mathcal{G},\mathbf{\Omega},\mathbf{F})$.

To facilitate a more comprehensive understanding of the theoretical results, we introduce the properties that are typically expected for local objective functions.

Definition 7 (*Properties of Objective Functions [124]*)**.** Consider an objective function $F:\mathbb{R}^n\to\mathbb{R}$.

1. Convexity: F is convex if the following inequality holds for all $x,y\in\mathbb{R}^n$ and for all $\varphi\in(0,1)$:
$$F(\varphi x+(1-\varphi)y)\le\varphi F(x)+(1-\varphi)F(y). \tag{21}$$
Furthermore, F is strongly convex if the above inequality becomes an equation for all $\varphi\in(0,1)$ only when $x=y$.
2. μ-Strong Convexity: When F is differentiable, for a given parameter $\mu\in\mathbb{R}_{>0}$, F is μ-strongly convex if the following inequality holds for all $x,y\in\mathbb{R}^n$:
$$(\nabla F(y)-\nabla F(x))^T(y-x)\ge\mu\|y-x\|^2. \tag{22}$$
3. L_f-Lipschitz Continuity: For a given parameter $L_f\in\mathbb{R}_{>0}$, F is Lipschitz continuous if there exists a constant $L_f\in\mathbb{R}_{>0}$ such that
$$|F(x)-F(y)|\le L_f\|x-y\|,\ \forall x,y\in\mathbb{R}^n. \tag{23}$$
4. L_g-Smoothness: When F is differentiable, for a given parameter $L_g\in\mathbb{R}_{>0}$, F is L_g-smooth if there exists a constant $L_g\in\mathbb{R}_{>0}$ such that
$$|\nabla F(x)-\nabla F(y)|\le L_g\|x-y\|,\ \forall x,y\in\mathbb{R}^n. \tag{24}$$

Among these properties, convexity, smoothness, and Lipschitz continuity are essential for ensuring the existence of optimal solutions and the convergence of optimization algorithms.

In the DPDO problem, the agents typically have privacy-sensitive information embedded in their (initial) states, objective functions, as well as constraints. Therefore, the adjacency relationship regarding the DPDO problem can be established by considering not only the (initial) states, as is the case in the DPC problem, but also the local objective functions and constraints. In the following, the definitions of two adjacent DO problems described based on their respective objective functions and constraints are presented.

Definition 8 (*Adjacency*)**.** Two DO problems $\mathcal{P}_a=(\mathcal{G}_a,\mathbf{\Omega}_a,\mathbf{F}_a)$ and $\mathcal{P}_b=(\mathcal{G}_b,\mathbf{\Omega}_b,\mathbf{F}_b)$ are adjacent, denoted by $\mathrm{Adj}(\mathcal{P}_a,\mathcal{P}_b)$, if exactly one of the following statements holds:

1. Adjacency relationship for objective functions [107]: Two DO problems $\mathcal{P}_a$ and $\mathcal{P}_b$ have identical parameters, with the only exception being a variation in at most one local objective function. To be more precise, $\mathcal{G}_a=\mathcal{G}_b$ and $\mathbf{\Omega}_a=\mathbf{\Omega}_b$; and there exists some $i_0\in\mathcal{V}$ such that $F_{ai_0}\neq F_{bi_0}$ and $F_{ai}=F_{bi}$ for all $i\in\mathcal{V}\backslash\{i_0\}$.
2. Adjacency relationship for constraints [125]: Two DO problems $\mathcal{P}_a$ and $\mathcal{P}_b$ have identical parameters, except for the constraints. Specifically, $\mathcal{G}_a=\mathcal{G}_b$ and $\mathbf{F}_a=\mathbf{F}_b$; and there exists some $i_0\in\mathcal{V}$ such that $\Omega_{ai_0}\neq\Omega_{bi_0}$ and $\Omega_{ai}=\Omega_{bi}$ for all $i\in\mathcal{V}\backslash\{i_0\}$.

To ensure DP in the context of the DO problem, it is common to impose additional requirements in the adjacency relationship. For instance, when defining the adjacency relationship for objective functions, it is common to mandate that all objective functions have uniformly bounded gradients [107] or exhibit similar gradient behaviors [106]. In the adjacency relationship for constraints, one may stipulate that the difference between two varying constraints is bounded by some nonnegative value σ, that is, there exists some $i_0\in\mathcal{V}$ such that $\mathrm{dist}\left(\Omega_{ai_0},\Omega_{bi_0}\right)\le\sigma$ and $\Omega_{ai}=\Omega_{bi}$ for all $i\in\mathcal{V}\backslash\{i_0\}$ [125].

Similar to the DPC problem setting, we assume that adversaries in the DPDO problem can spy on all communication channels between agents. In this regard, for a prescribed $T\in\mathbb{Z}_{\ge0}$, we denote the potential information set that adversaries accumulate over time horizon T given the DO problem $\mathcal{P}$ and the initial state $x(0)$ by $\mathcal{I}_{\mathcal{P},x(0)}(T)\in\mathbf{O}_T$, where $\mathbf{O}_T$ is the set of all potential accumulated information over time horizon T. Then we formalize the DP notion in the context of the DO problem as follows:

Definition 9 (*Differential Privacy*)**.** Consider a time horizon $T\in\mathbb{Z}_{\ge0}$ and a pair of parameters $\epsilon\in\mathbb{R}_{>0}$ and $\delta\in[0,1)$. An algorithm devised for the DO problem (20) is said to be (ϵ,δ)-differentially private over time horizon T if for any two adjacent $\mathcal{P}_a=(\mathcal{G}_a,\mathbf{\Omega}_a,\mathbf{F}_a)$ and $\mathcal{P}_b=(\mathcal{G}_b,\mathbf{\Omega}_b,\mathbf{F}_b)$, any initial state $x(0)$ and any set $\mathcal{O}_T\subseteq\mathbf{O}_T$, the following inequality holds:

$$\mathbb{P}\left\{\mathcal{I}_{\mathcal{P}_a,x(0)}\in\mathcal{O}_T\right\}\le e^{\epsilon}\mathbb{P}\left\{\mathcal{I}_{\mathcal{P}_b,x(0)}\in\mathcal{O}_T\right\}+\delta. \tag{25}$$

When $\delta=0$, the algorithm is ϵ-differentially private over time horizon T. Furthermore, if the inequality (7) holds for $T\to+\infty$, the devised algorithm is differentially private for the DO problem (20) over an infinite time horizon.

DPDO Problem

Devise a fully distributed algorithm integrated with a randomized mechanism such that the DO problem Eq. (20) is addressed while ensuring DP of agents' sensitive information.

4.2. Algorithms with non-amplifying noise perturbation

Most of the algorithms devised for resolving the DO problem stem from the consensus-based distributed (sub)gradient (CDG) algorithms. In the CDG algorithms, agents are propelled toward a common estimate of the optimal value by performing a consensus algorithm while descending along the local (sub)gradient direction of its respective convex objective function. When local constraints are considered in the DO problem, the solution at each update is projected onto the

constrained region, ensuring the feasibility of the solution. These algorithms have garnered considerable attention and popularity due to their advantageous combination of the (sub)gradient method and consensus algorithm—low computational and storage demands and high scalability.

A majority of the DPDO algorithms preserve DP by injecting noises with either decaying or constant (co)variance into shared messages or objective functions, with the majority treating local objective functions as privacy-sensitive information. This noise perturbation approach leads to an unavoidable privacy-utility trade-off, which remains a central focus of these algorithms.

In this subsection, we review the algorithms that use decaying noise perturbation according to the types of step sizes: diminishing and constant.

4.2.1. Diminishing step sizes

A number of algorithms with diminishing step sizes have been devised for a specific class of convex objective functions whose (sub)gradients are bounded. In these algorithms, the design of diminishing step sizes is vital and intricate, as it serves a crucial function in ensuring both convergence accuracy and DP. To illustrate, consider a fundamental CDG algorithm for the DO problem (20) with balanced digraphs and diminishing step sizes. At each update $k \in \mathbb{Z}_{\geq 0}$, agent $i \in \mathcal{V}$ receives state information from the neighbors and updates its state by:

$$x_i(k+1) = \sum_{j\in\mathcal{V}} [W]_{ij} x_j(k) - g(k) z_i(k), \tag{26}$$

where $g(k)$ is the diminishing step sizes; $z_i(k)$ represents the (sub)gradient of agent i. It is of importance to note that when $\omega \in \Omega \subseteq \mathbb{R}^n$ a projection of $x_i(k+1)$ is taken onto Ω that: $\mathrm{Proj}_{\Omega}\left\{x_i(k+1)\right\}$. It is worth noting that, in the CDG algorithm (26), the asymptotic convergence necessitates a diminishing step size that is non-summable but square-summable, which, however, brings difficulties in protecting DP over an infinite number of iterations.

The seminal work in [107] treated local objective functions as privacy-sensitive information and integrated state perturbation strategy into the projected CDG algorithm for the DPDO problem with undirected graphs and local convex constraints. To be precise, by substituting the state information $x_i(k)$ in (26) with the perturbed version $\hat{x}_i(k)$ in (27), the authors projected this vector on the common convex constraint.

$$\hat{x}_i(k) = x_i(k) + \theta_i(k), \ \forall k \in \mathbb{Z}_{\geq 0}, \forall i \in \mathcal{V}. \tag{27}$$

Here, each element of the random noises $\theta_i(k) \in \mathbb{R}^n$ follows i.i.d. Laplace distribution with zero mean and exponentially decaying variance to ensure convergence of the algorithm. Unlike conventional algorithms that use infinite-sum diminishing step sizes, the algorithm proposed in [107] considered summable step sizes, which is essential for guaranteeing DP over an infinite number of iterations, however concurrently introduces a steady-state error in the convergence accuracy. When objective functions are strongly convex with bounded gradients, the proposed algorithm in [107] sub-linearly converges to a random point while preserving ϵ-DP of objective functions over an infinite number of iterations. The convergence accuracy was characterized based on the expectation of the squared deviation of the states from the optimal point, which is inversely proportional to the square of a given privacy budget. This demonstrated a trade-off between the convergence accuracy and the privacy budget. The algorithm along with the state perturbation strategy proposed in [107] has been successfully adapted to address multiple distributed online optimization problems over various communication graphs, such as gossip-based undirected graphs [126], time-varying balanced digraphs [110], and (time-varying) unbalanced digraphs [111,112]. These adaptations attain ϵ-DP of objective functions either within a single iteration or over a finite number of iterations under the assumption that (sub)gradients are bounded. Moreover, an improvement upon [107] was made by [108], in which an event-triggered mechanism and the push-sum method were introduced to save resource consumption and counteract the impact of unbalanced digraphs on the convergence performance, respectively. They showed that adding exponentially decaying Laplacian noises to the states prior to sharing can preserve DP of both initial states and objective functions over an infinite number of iterations when the step sizes are summable.

A subsequent study in [109] presented a counterexample consistent with the observation in the above literature [107], revealing that solely perturbing shared information with asymptotically vanishing noises fails to preserve DP of objective functions over an infinite number of iterations when a noise-free distributed optimization algorithm is globally asymptotically stable. Motivated by this finding, the authors of [109] proposed an alternative randomized mechanism that injects well-designed functional Laplacian noises into *objective functions*. This approach facilitates bounding the difference between the probabilities of events associated with any pair of datasets by a function of the distance between the datasets. Although this method can achieve asymptotical convergence in the noise-free case, it should be mentioned that it only works for square-integrable objective functions, restricting the scope of its applications.

4.2.2. Constant step sizes

Note that the aforementioned algorithms employ diminishing step sizes, resulting in a slower convergence rate compared to those using constant step sizes. To enhance the convergence rate, a stream of CDG algorithms featuring constant step sizes, along with novel differentially private mechanisms, has been proposed for tackling the DPDO problem (20).

The authors of [113,114] considered constant step sizes and relaxed the requirement of objective functions from either convex objective functions with bounded (sub)gradients or square-integrable objective functions to general strongly convex and smooth objective functions. They confirmed the impossible result established in [109]—relying solely on state perturbation with vanishing random noises is inadequate for attaining simultaneous convergence and DP. As a result, they applied a state and direction perturbation strategy to ensure ϵ-DP of objective functions, and subsequently proposed a distributed optimization algorithm that combines the gradient method and the gradient tracking method. Specifically, for all $i \in \mathcal{V}$ and for all $k \in \mathbb{Z}_{\geq 0}$,

$$\begin{aligned}
\hat{x}_i(k) &= x_i(k) + \theta_i(k),\\
\hat{z}_i(k) &= z_i(k) + \zeta_i(k),\\
x_i(k+1) &= \sum_{j\in\mathcal{V}} [W]_{ij} \hat{x}_j(k) - g z_i(k),\\
z_i(k+1) &= \sum_{j\in\mathcal{V}} [W]_{ij} \hat{z}_j(k) + \nabla F_i(x_i(k+1)) - \nabla F_i(x_i(k)).
\end{aligned} \tag{28}$$

In this algorithm, $\theta_i(k)$ and $\zeta_i(k)$ are random noises for randomizing the state and direction of agent i, respectively. Each component of these noises follows exponentially decaying i.i.d. Laplace distribution. In addition, $g \in \mathbb{R}_{>0}$ refers to the constant step size for ensuring linear convergence while $z_i(k)$ is to track the averaged gradient, unlike (26) using the gradient. Assuming that objective functions are strongly convex, the algorithm developed in [113,114] attains both almost sure linear convergence without a steady-state error and DP of objective functions over an infinite number of iterations. Additionally, the convergence accuracy was derived, exhibiting the trade-off between DP and convergence accuracy.

Moving beyond solely noise perturbation mechanisms, the authors of [24] proposed a novel differentially private mechanism that combines direction state decomposition with direction perturbation to preserve DP of objective functions over a finite number of iterations. The basic idea is to decompose the local gradient into two components. One component is only available to the agent itself, while the other, after

being blurred by Laplacian noise with constant variance, is shared with the neighbors. A novel algorithm was subsequently developed in [24] that incorporates the aforementioned differentially private mechanism into a distributed push-pull gradient algorithm with constant step sizes to solve the DPDO problem over unbalanced digraphs and bounded gradients. The proposed algorithm in [24] enjoys linear convergence thanks to constant step sizes but has a steady-state error in convergence accuracy.

In addition, a line of research has approached the DPDO problem over undirected graphs by employing the alternating direction method of multipliers (ADMM) in combination with noise perturbation strategies. This ADMM technique integrates Lagrangian multipliers and quadratic penalty terms into objective functions and involves primal and dual updating, facilitating an accelerated convergence rate with less conservative convergence conditions at the expense of increased computational complexity [127,128]. In general, to preserve DP in ADMM algorithms, the noise perturbation strategies can be applied to either primal or dual variables, which are commonly referred to as primal perturbation (message perturbation) and dual perturbation (objective perturbation), respectively. To address a class of regularized empirical risk minimization (ERM) problems over undirected connected graphs while guaranteeing ϵ-differential privacy for each agent's training data (i.e., local objective functions) at a single iteration, the authors of [115] considered two types of noise perturbation strategies—primal perturbation and dual perturbation—in the ADMM algorithm, under the assumption of strongly convex and smooth objective functions. A comparative analysis of these two perturbation strategies was presented regarding their performance in the privacy-utility trade-off. Since then, various studies have been conducted to refine the proposed algorithm in [115] from distinct standpoints. The authors of [129] applied the dual perturbation technique in [115] to vehicular and hoc networks for DP preservation. The work in [116] developed a modified ADMM algorithm that endows an adaptive private penalty parameter to each agent and considered dual perturbation by introducing well-designed noises into the penalty term. The proposed algorithm strengthened privacy protection from a single iteration to a finite number of iterations and improved the convergence accuracy. To conserve the privacy budget and enhance computation efficiency, the authors of [117] devised a refined version of the algorithm in [116]. The proposed modified recycled ADMM algorithm enables the re-utilization of information from odd iterations in subsequent even iterations. Finally, the work in [130] devised a novel ADMM algorithm that adopts calibrated Gaussian noises in primal perturbation and applies a multi-step approximation technique in primal updating for improved accuracy.

4.3. Algorithms with amplifying noise perturbation

Recently, the authors of [106] have marked a crucial step forward in the literature on the differentially private DO problem, as their novel algorithms applicable to both undirected and unbalanced digraphs, for the first attempt, attain almost sure convergence to the optimal point while preserving ϵ-DP of objective functions over an infinite number of iterations. At the core of their algorithms is the introduction of additional diminishing parameters at every iteration to mitigate the impact of amplifying random noises that are persistently injected into the shared message on the convergence accuracy. Their algorithms successfully circumvent the need for summable step sizes in the updating process, which serves as a key factor in the algorithm proposed by [107] for safeguarding DP over an infinite number of iterations while also bringing in an inherent convergence error. Specifically, for the unconstrained DO problem over undirected graphs and convex, the following algorithm was proposed in [106]: for all $i \in \mathcal{V}$ and for all $k \in \mathbb{Z}_{\geq 0}$,

$$\begin{aligned} \hat{x}_i(k) &= x_i(k) + \theta_i(k), \\ x_i(k+1) &= x_i(k) + \sum_{j \in \mathcal{N}_i^{\text{in}}} \hat{g}(k)[\mathcal{A}]_{ij}(\hat{x}_j(k) - x_i(k)) \\ &\quad - g(k)\nabla F_i(x_i(k)). \end{aligned} \tag{29}$$

In this algorithm, a distinct feature is that each element of random noise $\theta_i(k)$ injected to the shared state is from i.i.d. Laplace distribution with increasing variance, which serves to ensure ϵ-DP of objectives over an infinite number of iterations. Moreover, $g(k) \in \mathbb{R}_{>0}$ is non-summable diminishing step size and $\hat{g}(k) \in \mathbb{R}_{>0}$ is the non-summable weakening factor that attenuates non-decaying perturbation noises $\theta_i(k)$. With the proposed algorithm over undirected graphs and assuming that objective functions are convex and smooth, agents commonly converge to an optimal point almost surely while ϵ-DP of objective functions is preserved over an infinite number of iterations, when step sizes, weakening factors, and injected noises are properly designed. Furthermore, weakening factors have been integrated into the push-pull gradient algorithm to solve the unbalanced digraph case. It should be mentioned that the main drawback of the algorithms proposed in [109] is their slower convergence rate compared to those without weakening factors.

4.4. Application to distributed resource allocation

Recently, some literature has customized the aforementioned algorithms, primarily developed for solving the DO problem (20), to tackle the optimal distributed resource allocation (DRA) problem while ensuring DP of local power generation, demands, and objective functions. Central to most of these studies is the treatment of the optimal DRA problem in the corresponding dual problem as formulated in (20) with shared message perturbed with decaying random noises, under the assumption that there are no dual gap and nonempty dual optimal set. In this subsection, we review the algorithms for addressing the differentially private optimal DRA problem, categorizing them by the type of step sizes: constant and diminishing.

DRA Problem

$$\begin{aligned} &\min \sum_{i \in \mathcal{V}} C_i(\omega_i) \\ &\text{s.t.} \sum_{i \in \mathcal{V}} \omega_i = \sum_{i \in \mathcal{V}} D_i, \\ &\quad \omega_i \in \Omega_i, \ \forall i \in \mathcal{V}, \end{aligned} \tag{30}$$

with ω_i, $C_i : \mathbb{R} \to \mathbb{R}$, and D_i represent the power generation, the local objective function and local demand associated with the i-th generator, respectively; Ω_i is a closed and convex set that defines the constraint of the i-th generator.

Before exhibiting relevant algorithms, we establish the framework for transforming the optimal DRA problem into the DO problem. Consider the above optimal distributed resource allocation (DRA) problem, which aims to design an algorithm that cooperatively minimizes the sum of local objective functions while satisfying the overall demand and adhering to specific output constraints of each agent without relying on a central aggregator.

The optimal DRA problem formulated in (30) has extensive practical applications, among which are the economic dispatch problem in smart grids where Ω_i is a box constraint denoted as $\Omega_i = \{\omega_i : \underline{\omega}_i \leq \omega \leq \bar{\omega}_i\}$. Let $\omega = (\omega_1, \ldots, \omega_N)$ and consider the Lagrangian function $\mathcal{L}(\omega, \lambda) = \sum_{i \in \mathcal{V}} C_i(\omega_i) - \lambda \left(\sum_{i \in \mathcal{V}} \omega_i - \sum_{i \in \mathcal{V}} D_i \right)$ with λ being the dual variable. Then the optimal DRA problem (30) is readily transformed into the following dual optimization problem:

$$\max_{\lambda} \sum_{i \in \mathcal{V}} F_i(\lambda) \tag{31}$$

with $F_i(\lambda) = \min_{\omega_i \in \Omega_i} C_i(\omega_i) - \lambda(\omega_i - D_i)$.

- *Algorithms with diminishing step sizes:* A few algorithms with diminishing step sizes have been proposed for solving the optimal

DRA problem (30) with ϵ-DP safeguarded. These algorithms follow the noise perturbation strategy in [107] that injects exponentially decaying Laplacian noises with zero mean into the shared states in the dual updating, only preserving DP over a finite number of iterations or at a single update. Furthermore, there is a trade-off between the privacy budget and convergence accuracy for these algorithms: as the number of iterations increases, the privacy budget may increase while the convergence accuracy improves. The authors of [118,119] proposed a differentially private mechanism that perturbs power generation with exponentially decaying Laplacian noises at each iteration. For a specific class of optimal DRA problems featuring quadratic objectives with bounded gradients and undirected graphs, the proposed mechanism effectively protects ϵ-DP of both objective functions and local demands (constraints) over a finite number of iterations. When time-varying unbalanced digraphs are considered, the work in [131] applied the push-sum method to counteract the unbalance of digraphs on the convergence performance. It ensures ϵ-DP of local demands over a finite number of iterations or at a single update by injecting diminishing Laplacian noises into dual states.

• *Algorithms with constant step sizes:* To realize faster convergence speed and better privacy protection, some researchers have explored the use of constant step sizes instead of diminishing step sizes in their algorithms. In particular, the authors of [120] focused on the undirected graph case for the general optimal DRA problem. They borrowed the DPDO algorithm (28) in their previous work [113] with constant step sizes for dual updating, in which both states and gradients are masked with exponentially decaying Laplacian noises and the gradient tracking approach was applied for monitoring the deviation of the total generation from total demands. Under the assumption that objective functions are strongly convex and smooth, the proposed algorithm is able to achieve linear convergence and preserve ϵ-DP of objective functions over an infinite number of iterations simultaneously. An extension of this work to more general constraints in the form as $\sum_{i\in\mathcal{V}} A_i\omega_i = \sum_{i\in\mathcal{V}} D_i, \forall i \in \mathcal{V}$ can be found in [121].

In addition to addressing the general form of the differentially private optimal DRA problem, some algorithms have specifically targeted quadratic objective functions or box constraints within the context of undirected graphs. This focus allows for resource conservation [132], the handling of time-varying objective functions [133], and the accommodation of multiple heterogeneous generators [134], while ensuring ϵ-DP of power generation at a single update. Moreover, the authors of [122] investigated this problem with box constraints and unbalanced digraphs. Inspired by the differentially private mechanism proposed in [24], they combined noise perturbation with gradient-tracker decomposition in the push-pull gradient tracking algorithm for dual updating. The devised algorithm is able to attain linear convergence while ensuring ϵ-DP of objective functions at a single iteration when objective functions are strongly convex and smooth.

Note that previously mentioned algorithms are infeasible in dealing with situations involving time delays, which is, however, prevalent in most practical applications of MASs. In an effort to overcome this limitation, the authors of [123] took into consideration objective functions with heterogeneous time delays and box constraints for the optimal DRA problem (30). Instead of approaching the optimal DRA problem through dual optimization, they developed a novel algorithm that applies a predictive scheme to estimate the missing states between two consecutive iterations and subsequently integrated it into the CDG algorithm. Furthermore, the exchanged gradient information is obfuscated by exponentially decaying Laplacian noises, adding a layer of privacy protection to the process. Specifically, for all $i \in \mathcal{V}$ and for all $k \in \mathbb{Z}_{\geq 0}$,

$$\begin{aligned} \widetilde{F}_i(k) &= \nabla F_i\left(\hat{\omega}_i(k \mid k-\tau_i)\right) + \theta_i(k), \\ \omega_i(k+1) &= \omega_i(k) - g\sum_{j\in\mathcal{V}}[L]_{ij}\nabla\widetilde{F}_j(k), \end{aligned} \tag{32}$$

in which $F_i(\omega_i) = C_i(\omega_i) - \frac{1}{h}\left[\log(\omega_i - \underline{\omega}_i) + \log(\bar{\omega}_i - \omega_i)\right]$ is the penalized objective function that integrates box constraints into objectives by the logarithmic barrier function, in which $h \in \mathbb{R}_{>0}$ modulates the degree of penalization. Moreover, $\tau_i \in \mathbb{R}_{\geq 0}$ and $g \in \mathbb{R}_{>0}$ denote the time delay and constant step sizes concerning ith generator, respectively; $\hat{\omega}_i(k \mid k-\tau_i)$ is the predictor of ith generator based on the available information up to $k-\tau_i$; $\theta_i(k), \forall i \in \mathcal{V}$, are i.i.d. from exponentially decaying Laplacian noises with zero mean. Under the assumption that penalized objectives are twice differentiable and strongly convex, the proposed algorithm in [123] guarantees both linear convergence and ϵ-DP of local power generation, i.e., state, over an infinite number of iterations. Moreover, the algorithm accuracy and privacy budget were characterized.

4.5. Discussion on trade-off

The implementation of differentially private mechanisms heavily relies on the injection of random noises, which, however, impedes the achievement of the desired control performance. The more noise is injected, the more privacy is preserved, but the less performance of the control algorithms will be achieved. Just consider two extreme scenarios. In the first extreme scenario, where the maximal amount of noise is injected into the shared information or no information is shared between the agents, the privacy of the agents is strongly preserved. However, achieving the desired control performance becomes impossible. Conversely, in the second extreme scenario, where no noise is injected into the shared information, the desired control performance is guaranteed accurately and effectively. However, the privacy of the agents is entirely breached. Therefore, the core challenge of implementing differentially private mechanisms into distributed MAS control is how to balance the desired control performance and the privacy protection strength.

In the context of DPC algorithms, the main trade-off involves balancing consensus accuracy and privacy protection strength or balancing convergence speed and privacy protection strength. Specifically, in static average consensus, this trade-off is manifested as the ability to achieve an accurate consensus while preserving privacy. As demonstrated in [22,82,97], the consensus accuracy is inversely proportional to the protection level of DP. For dynamic average consensus, accurate consensus can be guaranteed, as shown in [86]. However, a lower convergence speed is associated with a higher level of privacy protection.

The trade-off faced by DPDO algorithms is analogous to that in DPC algorithms. This is primarily because greater noise magnitudes yield stronger privacy protection at the expense of higher optimality errors. Striking a balance between privacy protection and optimization accuracy is especially challenging without parameters to weaken the influence of noise on optimality accuracy. For instance, the results in [118,119] showed that the level of privacy protection decreases with the number of iterations increases, while the optimality accuracy improves.

5. Conclusions and potential research directions

In this paper, we have surveyed the integration of DP into consensus and distributed optimization, two interrelated and crucial research issues in distributed MAS control. First, we have presented the typical features and modeling of MASs from the control theory standpoint and identified relevant research topics with an emphasis on consensus and distributed optimization. With this knowledge at hand, we have articulated the rationale behind incorporating differentially private mechanisms to safeguard the privacy of distributed MAS control. Subsequently, we have expounded on the fundamental principles of DP and discussed the primary challenge of striking a balance between utility and privacy when integrating DP into distributed MAS control. With a solid understanding of the motivations and challenges, we carried out an in-depth investigation of the state-of-the-art techniques that have been developed for preserving DP in both consensus and distributed

optimization. Furthermore, we discussed the trade-offs involved in implementing these privacy-preserving mechanisms.

DP plays an essential role in safeguarding privacy for consensus and distributed MAS control. However, the corresponding techniques in these two problems are still in their early stages of research and warrant further investigation. We outline potential improvements on existing results and research directions in the future as follows:

- *Presence of communication imperfections:* In practical scenarios, MASs frequently encounter imperfect communication, including time delays, packet losses, and time-varying communication topologies, resulting from limited resources and environmental interference. These imperfections have a significant impact on the performance of distributed MAS control. Although a limited number of studies have been directed toward addressing these challenges, such as [123], there is a continued need for further investigation to attain the desired control performance in various practical circumstances.
- *Exploration of MASs with complex dynamics:* One common characteristic shared by existing differential private algorithms is that only agents with linear dynamics are considered. However, real-world systems usually exhibit complex behaviors that cannot be modeled by linear systems. Therefore, it would be worth investigating the application of DP in complex and nonlinear MAS models, taking into account various dynamic behaviors, interactions, and uncertainties present in real-world systems.
- *Integration of learning-based control:* The existing DPC algorithms were proposed by model-based methodologies. However, this approach may be inadequate when the dynamics of agents in reality is excessively complicated to be precisely modeled or remains completely unknown. In recent years, learning-based control, such as reinforcement learning control and deep learning control, has proved its potential for mitigating this limitation for the privacy-free consensus problem by utilizing data collected from real systems to devise a control scheme. Therefore, an intriguing future research direction involves integrating differentially private mechanisms into learning-based control schemes to solve the DPC problem of MASs without precise system knowledge.
- *Resilience against cyber-attacks:* In addition to facing privacy threats, the inherently distributed configuration of MASs also exposes them to an environment susceptible to various cyber-attacks, including but not limited to denial of service (DoS) attacks, deception attacks, and replay attacks. Moreover, adversaries can exploit the information intercepted from communication channels to launch more sophisticated attacks. Therefore, it is crucial to design a differentially private control algorithm that is resilient against cyber-attacks in distributed MAS control. Regrettably, only a handful of studies, such as [67,83], have considered (differential) privacy preservation and resilience against cyber-attacks in the control algorithm design of MASs, indicating a need for further research in this domain.
- *Refinement and extension of differential privacy:* The critical bottleneck of applying DP to distributed MAS control is its applicability only to the discrete-time information stream, although some studies have attempted to apply DP to continuous-time MASs by considering a discrete-time communication strategy [97]. Consequently, refining and extending the concept of DP for continuous-time MASs can significantly enhance its applicability and relevance in dealing with diverse MAS control applications.

CRediT authorship contribution statement

Yamin Wang: Writing – original draft, Methodology, Investigation. **Hong Lin:** Writing – review & editing, Supervision. **James Lam:** Writing – review & editing, Supervision. **Ka-Wai Kwok:** Writing – review & editing.

Declaration of competing interest

We confirm that this work is original and has not been published elsewhere nor is it currently under consideration for publication elsewhere. We also declare that there is no conflict of interest regarding the publication of this paper. All authors have checked the manuscript and have agreed to the submission.

Data availability

No data was used for the research described in the article.

Acknowledgments

This work was supported by Shenzhen Polytechnic University Research Fund under Grant 602331015PQ; General Research Fund under Grants 17202922 and 17209021; National Science Foundation China under Grant 62273286; Shenzhen-Hong Kong-Macau Technology Research Programme under Grant SGDX20230821091559019.

References

[1] Y. Li, C. Tan, A survey of the consensus for multi-agent systems, Syst. Sci. Control Eng. 7 (1) (2019) 468–482.
[2] C.W. Reynolds, Flocks, herds, and schools: A distributed behavioral model, in: Proceedings of the 14th Annual Conference on Computer Graphics and Interactive Techniques, SIGGRAPH'87, Association for Computing Machinery, New York, NY, USA, 1998, pp. 273–282.
[3] T. Vicsek, A. Czirók, E. Ben-Jacob, I. Cohen, O. Shochet, Novel type of phase transition in a system of self-driven particles, Phys. Rev. Lett. 75 (6) (1995) 1226.
[4] R. Olfati-Saber, R. Murray, Consensus problems in networks of agents with switching topology and time-delays, IEEE Trans. Autom. Control 49 (9) (2004) 1520–1533.
[5] H. Ishii, Y. Wang, S. Feng, An overview on multi-agent consensus under adversarial attacks, Annu. Rev. Control 53 (2022) 252–272.
[6] D. Ding, Q.-L. Han, Z. Wang, X. Ge, A survey on model-based distributed control and filtering for industrial cyber-physical systems, IEEE Trans. Ind. Inform. 15 (5) (2019) 2483–2499.
[7] L. Zou, Z. Wang, J. Hu, Y. Liu, X. Liu, Communication-protocol-based analysis and synthesis of networked systems: Progress, prospects and challenges, Int. J. Syst. Sci. 52 (14) (2021) 3013–3034.
[8] A. Amirkhani, A.H. Barshooi, Consensus in multi-agent systems: A review, Artif. Intell. Rev. 55 (5) (2022) 3897–3935.
[9] G. Bao, L. Ma, X. Yi, Recent advances on cooperative control of heterogeneous multi-agent systems subject to constraints: A survey, Syst. Sci. Control Eng. 10 (1) (2022) 539–551.
[10] Y.-A. Wang, B. Shen, L. Zou, Q.-L. Han, A survey on recent advances in distributed filtering over sensor networks subject to communication constraints, Int. J. Netw. Dyn. Intell. 2 (2) (2023) 100007.
[11] I. Krontiris, F. Freiling, T. Dimitriou, Location privacy in urban sensing networks: Research challenges and directions [Security and privacy in emerging wireless networks], IEEE Wirel. Commun. 17 (2010) 30–35.
[12] M. Ye, Y. Qin, A. Govaert, B.D. Anderson, M. Cao, An influence network model to study discrepancies in expressed and private opinions, Automatica 107 (2019) 371–381.
[13] H. Cai, G. Hu, Distributed tracking control of an interconnected leader–follower multiagent system, IEEE Trans. Autom. Control 62 (7) (2017) 3494–3501.
[14] P. McDaniel, S. McLaughlin, Security and privacy challenges in the smart grid, IEEE Secur. Privacy 7 (3) (2009) 75–77.
[15] D. Hahn, A. Munir, V. Behzadan, Security and privacy issues in intelligent transportation systems: Classification and challenges, IEEE Intell. Transp. Syst. Mag. 13 (1) (2021) 181–196.
[16] M.U. Hassan, M.H. Rehmani, J. Chen, Differential privacy techniques for cyber physical systems: A survey, IEEE Commun. Surv. Tutor. 22 (1) (2019) 746–789.
[17] C. Dwork, A. Roth, The algorithmic foundations of differential privacy, Found. Trends Theor. Comput. Sci. 9 (3–4) (2013) 211–407.
[18] C. Dwork, F. McSherry, K. Nissim, A. Smith, Calibrating noise to sensitivity in private data analysis, in: Theory of Cryptography: Third Theory of Cryptography Conference, Springer, New York, USA, 2006, pp. 265–284.
[19] A. Nedić, J. Liu, Distributed optimization for control, Annu. Rev. Control, Robotics, Auton. Syst. 1 (1) (2018) 77–103.
[20] Z. Huang, S. Mitra, G. Dullerud, Differentially private iterative synchronous consensus, in: Proceedings of the 2012 ACM Workshop on Privacy in the Electronic Society, 2012, pp. 81–90.

[21] Y. Wang, Z. Huang, S. Mitra, G.E. Dullerud, Differential privacy in linear distributed control systems: Entropy minimizing mechanisms and performance tradeoffs, IEEE Trans. Control Netw. Syst. 4 (1) (2017) 118–130.

[22] E. Nozari, P. Tallapragada, J. Cortés, Differentially private average consensus: Obstructions, trade-offs, and optimal algorithm design, Automatica 81 (2017) 221–231.

[23] K. Yazdani, A. Jones, K. Leahy, M. Hale, Differentially private LQ control, IEEE Trans. Autom. Control 68 (2) (2023) 1061–1068.

[24] X. Chen, L. Huang, L. He, S. Dey, L. Shi, A differentially private method for distributed optimization in directed networks via state decomposition, IEEE Trans. Control Netw. Syst. (2023) 1–11.

[25] Z.-H. Pang, L.-Z. Fan, H. Guo, Y. Shi, R. Chai, J. Sun, G.-P. Liu, Security of networked control systems subject to deception attacks: A survey, Int. J. Syst. Sci. 53 (16) (2022) 3577–3598.

[26] Y. Zhang, Y.-P. Tian, Consensus of data-sampled multi-agent systems with random communication delay and packet loss, IEEE Trans. Autom. Control 55 (4) (2010) 939–943.

[27] L. Yu, Y. Cui, Y. Liu, N.D. Alotaibi, F.E. Alsaadi, Sampled-based consensus of multi-agent systems with bounded distributed time-delays and dynamic quantisation effects, Int. J. Syst. Sci. 53 (11) (2022) 2390–2406.

[28] L. Ding, Q.-L. Han, X. Ge, X.-M. Zhang, An overview of recent advances in event-triggered consensus of multiagent systems, IEEE Trans. Cybern. 48 (4) (2018) 1110–1123.

[29] F. Han, J. Liu, J. Li, J. Song, M. Wang, Y. Zhang, Consensus control for multi-rate multi-agent systems with fading measurements: The dynamic event-triggered case, Syst. Sci. Control Eng. 11 (1) (2023) 2158959.

[30] K. Chen, C. Yan, Q. Ren, J. Wang, Dynamic event-triggered leader-following consensus of nonlinear multi-agent systems with measurement noises, IET Control Theory Appl. 17 (10) (2023) 1367–1380.

[31] F. Chen, W. Ren, On the control of multi-agent systems: A survey, Found. Trends Syst. Control 6 (4) (2019) 339–499.

[32] X. Ge, Q.-L. Han, X.-M. Zhang, L. Ding, F. Yang, Distributed event-triggered estimation over sensor networks: A survey, IEEE Trans. Cybern. 50 (3) (2019) 1306–1320.

[33] X.-M. Zhang, Q.-L. Han, X. Ge, D. Ding, L. Ding, D. Yue, C. Peng, Networked control systems: A survey of trends and techniques, IEEE/CAA J. Autom. Sin. 7 (1) (2019) 1–17.

[34] X. Ge, Q.-L. Han, L. Ding, Y.-L. Wang, X.-M. Zhang, Dynamic event-triggered distributed coordination control and its applications: A survey of trends and techniques, IEEE Trans. Syst., Man, Cybern.: Syst. 50 (9) (2020) 3112–3125.

[35] M.A. Joordens, M. Jamshidi, Consensus control for a system of underwater swarm robots, IEEE Syst. J. 4 (1) (2010) 65–73.

[36] V. Strobel, E. Castelló Ferrer, M. Dorigo, Blockchain technology secures robot swarms: A comparison of consensus protocols and their resilience to Byzantine robots, Front. Robotics AI 7 (2020) 54.

[37] S. Kar, G. Hug, J. Mohammadi, J.M.F. Moura, Distributed state estimation and energy management in smart grids: A consensus+ innovations approach, IEEE J. Sel. Top. Sign. Proces. 8 (6) (2014) 1022–1038.

[38] J.J. Liu, J. Lam, B. Zhu, X. Wang, Z. Shu, K.-W. Kwok, Nonnegative consensus tracking of networked systems with convergence rate optimization, IEEE Trans. Neural Netw. Learn. Syst. 33 (12) (2021) 7534–7544.

[39] Y. Dong, Q. Zha, H. Zhang, G. Kou, H. Fujita, F. Chiclana, E. Herrera-Viedma, Consensus reaching in social network group decision making: Research paradigms and challenges, Knowl.-Based Syst. 162 (2018) 3–13.

[40] U. Niethammer, M. James, S. Rothmund, J. Travelletti, M. Joswig, UAV-based remote sensing of the Super-Sauze landslide: Evaluation and results, Eng. Geol. 128 (2012) 2–11.

[41] R. Parikh, P. Krasucki, Communication, consensus, and knowledge, J. Econom. Theory 52 (1) (1990) 178–189.

[42] D. Acemoğlu, G. Como, F. Fagnani, A. Ozdaglar, Opinion fluctuations and disagreement in social networks, Math. Oper. Res. 38 (1) (2013) 1–27.

[43] C. Deng, W.-W. Che, Z.-G. Wu, A dynamic periodic event-triggered approach to consensus of heterogeneous linear multiagent systems with time-varying communication delays, IEEE Trans. Cybern. 51 (4) (2020) 1812–1821.

[44] W. Jiang, K. Liu, T. Charalambous, Multi-agent consensus with heterogeneous time-varying input and communication delays in digraphs, Automatica 135 (2022) 109950.

[45] B.J. Karaki, M.S. Mahmoud, Scaled consensus design for multiagent systems under DoS attacks and communication-delays, J. Franklin Inst. 358 (7) (2021) 3901–3918.

[46] J. Wang, X. Luo, J. Yan, X. Guan, Event-triggered consensus control for second-order multi-agent system subject to saturation and time delay, J. Franklin Inst. 358 (9) (2021) 4895–4916.

[47] J. Guo, W. Wang, W. Zou, Z. Xiang, Consensus tracking control for nonlinear multiagent systems with asymmetric state constraints and input delays, J. Franklin Inst. 359 (16) (2022) 8579–8597.

[48] Y. Du, Y. Wang, Z. Zuo, Bipartite consensus for multi-agent systems with noises over Markovian switching topologies, Neurocomputing 419 (2021) 295–305.

[49] Y. Li, X. Liu, H. Liu, C. Du, P. Lu, Distributed dynamic event-triggered consensus control for multi-agent systems under fixed and switching topologies, J. Franklin Inst. 358 (8) (2021) 4348–4372.

[50] X. Jin, Y. Shi, Y. Tang, H. Werner, J. Kurths, Event-triggered fixed-time attitude consensus with fixed and switching topologies, IEEE Trans. Autom. Control 67 (8) (2021) 4138–4145.

[51] X.-J. Peng, Y. He, Consensus of multiagent systems with time-varying delays and switching topologies based on delay-product-type functionals, IEEE Trans. Cybern. (2022).

[52] L. Xu, Y. Mo, L. Xie, Distributed consensus over Markovian packet loss channels, IEEE Trans. Autom. Control 65 (1) (2019) 279–286.

[53] G. Chen, Y. Kang, C. Zhang, S. Chen, Consensus of discrete-time multi-agent systems over packet dropouts channels, J. Franklin Inst. 358 (13) (2021) 6684–6704.

[54] J. Zhang, K. You, K. Cai, Distributed dual gradient tracking for resource allocation in unbalanced networks, IEEE Trans. Signal Process. 68 (2020) 2186–2198.

[55] S. Boyd, Distributed optimization and statistical learning via the alternating direction method of multipliers, Found. Trends Mach. Learn. 3 (1) (2010) 1–122.

[56] Y. Zhang, X. Lin, DiSCO: Distributed optimization for self-concordant empirical loss, in: The 32nd International Conference on Machine Learning, PMLR, Lille, France, 2015, pp. 362–370.

[57] A. Machanavajjhala, D. Kifer, J. Gehrke, M. Venkitasubramaniam, L-diversity: Privacy beyond k-anonymity, ACM Trans. Knowl. Discov. Data (TKDD) 1 (1) (2007) 3–es.

[58] A. Narayanan, V. Shmatikov, Robust de-anonymization of large sparse datasets, in: 2008 IEEE Symposium on Security and Privacy, (Sp 2008), IEEE, 2008, pp. 111–125.

[59] M. Douriez, H. Doraiswamy, J. Freire, C.T. Silva, Anonymizing NYC taxi data: Does it matter? in: 2016 IEEE International Conference on Data Science and Advanced Analytics, DSAA, IEEE, Montreal, QC, Canada, 2016, pp. 140–148.

[60] R. Venkatesaramani, B.A. Malin, Y. Vorobeychik, Re-identification of individuals in genomic datasets using public face images, Sci. Adv. 7 (47) (2021) eabg3296.

[61] C. Gao, Z. Wang, X. He, H. Dong, Encryption–decryption-based consensus control for multi-agent systems: Handling actuator faults, Automatica 134 (2021) 109908.

[62] C. Gao, Z. Wang, X. He, H. Dong, Fault-tolerant consensus control for multiagent systems: An encryption-decryption scheme, IEEE Trans. Autom. Control 67 (5) (2022) 2560–2567.

[63] C.N. Hadjicostis, Privary preserving distributed average consensus via homomorphic encryption, in: 2018 IEEE Conference on Decision and Control, CDC, IEEE, Miami Beach, FL, USA, 2018, pp. 1258–1263.

[64] C. Zhang, Y. Wang, Enabling privacy-preservation in decentralized optimization, IEEE Trans. Control Netw. Syst. 6 (2) (2019) 679–689.

[65] J. Domingo-Ferrer, O. Farras, J. Ribes-González, D. Sánchez, Privacy-preserving cloud computing on sensitive data: A survey of methods, products and challenges, Comput. Commun. 140 (2019) 38–60.

[66] Y. Wang, Privacy-preserving average consensus via state decomposition, IEEE Trans. Autom. Control 64 (11) (2019) 4711–4716.

[67] Y. Zhang, Z. Peng, G. Wen, J. Wang, T. Huang, Privacy preserving-based resilient consensus for multi-agent systems via state decomposition, IEEE Trans. Control Netw. Syst. (2022) 1–12.

[68] Y. Wang, J. Lu, W.X. Zheng, K. Shi, Privacy-preserving consensus for multi-agent systems via node decomposition strategy, IEEE Trans. Circuits Syst. I. Regul. Pap. 68 (8) (2021) 3474–3484.

[69] J. Zhang, J. Lu, J. Liang, K. Shi, Privacy-preserving average consensus in multiagent systems via partial information transmission, IEEE Trans. Syst., Man, Cybern.: Syst. 53 (5) (2023) 2781–2791.

[70] W. Zhang, Z. Zuo, Y. Wang, G. Hu, How much noise suffices for privacy of multi-agent systems? IEEE Trans. Autom. Control (2022) 1–16.

[71] Y. Mo, R.M. Murray, Privacy preserving average consensus, IEEE Trans. Autom. Control 62 (2) (2017) 753–765.

[72] M. Ruan, H. Gao, Y. Wang, Secure and privacy-preserving consensus, IEEE Trans. Autom. Control 64 (10) (2019) 4035–4049.

[73] J. He, L. Cai, P. Cheng, J. Pan, L. Shi, Consensus-based data-privacy preserving data aggregation, IEEE Trans. Autom. Control 64 (12) (2019) 5222–5229.

[74] I. Mironov, Rényi differential privacy, in: 2017 IEEE 30th Computer Security Foundations Symposium, CSF, IEEE, Santa Barbara, CA, USA, 2017, pp. 263–275.

[75] M. Bun, T. Steinke, Concentrated differential privacy: Simplifications, extensions, and lower bounds, in: Theory of Cryptography Conference, Springer, 2016, pp. 635–658.

[76] K. Chatzikokolakis, M.E. Andrés, N.E. Bordenabe, C. Palamidessi, Broadening the scope of differential privacy using metrics, in: 13th International Symposium on Privacy Enhancing Technologies, Springer, Bloomington, IN, USA, 2013, pp. 82–102.

[77] I. Wagner, D. Eckhoff, Technical privacy metrics: A systematic survey, ACM Comput. Surv. 51 (3) (2018) 1–38.

[78] Y. Zhao, J. Chen, A survey on differential privacy for unstructured data content, ACM Comput. Surv. 54 (10s) (2022) 1–28.

[79] P. Kairouz, S. Oh, P. Viswanath, The composition theorem for differential privacy, in: The 32nd International Conference on Machine Learning, PMLR, Lille, France, 2015, pp. 1376–1385.

[80] Q. Geng, P. Viswanath, The optimal noise-adding mechanism in differential privacy, IEEE Trans. Inform. Theory 62 (2) (2016) 925–951.
[81] J. He, L. Cai, X. Guan, Differential private noise adding mechanism and its application on consensus algorithm, IEEE Trans. Signal Process. 68 (2020) 4069–4082.
[82] E. Nozari, P. Tallapragada, J. Cortés, Differentially private average consensus with optimal noise selection, IFAC-PapersOnLine 48 (22) (2015) 203–208.
[83] D. Fiore, G. Russo, Resilient consensus for multi-agent systems subject to differential privacy requirements, Automatica 106 (2019) 18–26.
[84] G. Grimmett, D. Stirzaker, Probability and Random Processes, Oxford University Press, 2020.
[85] X. Mao, Stochastic Differential Equations and Applications, Elsevier, 2007.
[86] Y. Wang, A robust dynamic average consensus algorithm that ensures both differential privacy and accurate convergence, 2023, arXiv preprint arXiv:2211.07791.
[87] Z. Zuo, R. Tian, Q. Han, Y. Wang, W. Zhang, Differential privacy for bipartite consensus over signed digraph, Neurocomputing 468 (2022) 11–21.
[88] W. Chen, Z. Wang, J. Hu, G.-P. Liu, Differentially private average consensus with logarithmic dynamic encoding–decoding scheme, IEEE Trans. Cybern. (2023) 1–12.
[89] T. Dong, X. Bu, W. Hu, Distributed differentially private average consensus for multi-agent networks by additive functional Laplace noise, J. Franklin Inst. 357 (6) (2020) 3565–3584.
[90] L. Gao, S. Deng, W. Ren, Differentially private consensus with an event-triggered mechanism, IEEE Trans. Control Netw. Syst. 6 (1) (2018) 60–71.
[91] L. Gao, S. Deng, W. Ren, C. Hu, Differentially private consensus with quantized communication, IEEE Trans. Cybern. 51 (8) (2019) 4075–4088.
[92] X.-K. Liu, Y.-W. Wang, J.-W. Xiao, M. Chi, Z.-W. Liu, Concentrated differentially private average consensus algorithm for a discrete-time network with heterogeneous dynamics, J. Franklin Inst. 359 (4) (2022) 1655–1676.
[93] Y. Pu, Differential privacy for distributed consensus with partial observations, in: 2020 IEEE 16th International Conference on Control & Automation, ICCA, IEEE, Sapporo, Hokkaido, Japan, 2020, pp. 88–93.
[94] Y. Wang, J. Lam, H. Lin, Differentially private average consensus with general directed graphs, Neurocomputing 458 (2021) 87–98.
[95] A. Wang, X. Liao, H. He, Event-triggered differentially private average consensus for multi-agent network, IEEE/CAA J. Autom. Sin. 6 (1) (2019) 75–83.
[96] Y. Wang, J. Lam, H. Lin, Differentially private average consensus for networks with positive agents, IEEE Trans. Cybern. (2023) 1–14.
[97] X.-K. Liu, J.-F. Zhang, J. Wang, Differentially private consensus algorithm for continuous-time heterogeneous multi-agent systems, Automatica 122 (2020) 109283.
[98] S.S. Kia, B. Van Scoy, J. Cortes, R.A. Freeman, K.M. Lynch, S. Martinez, Tutorial on dynamic average consensus: The problem, its applications, and the algorithms, IEEE Control Syst. Mag. 39 (3) (2019) 40–72.
[99] W. Zhang, B.-C. Wang, Y. Liang, Differentially private consensus for second-order multiagent systems with quantized communication, IEEE Trans. Neural Netw. Learn. Syst. (2022) 1–13.
[100] Y. Wang, J. Lam, H. Lin, Consensus of linear multivariable discrete-time multiagent systems: Differential privacy perspective, IEEE Trans. Cybern. 52 (12) (2022) 13915–13926.
[101] T. Li, L. Xie, Distributed coordination of multi-agent systems with quantized-observer based encoding-decoding, IEEE Trans. Autom. Control 57 (12) (2012) 3023–3037.
[102] M.E. Valcher, P. Misra, On the consensus and bipartite consensus in high-order multi-agent dynamical systems with antagonistic interactions, Systems Control Lett. 66 (2014) 94–103.
[103] J. Ma, J. Hu, Safe consensus control of cooperative-competitive multi-agent systems via differential privacy, Kybernetika (2022) 426–439.
[104] J. Wang, J. Ke, J.-F. Zhang, Differentially private bipartite consensus over signed networks with time-varying noises, 2022, arXiv preprint arXiv:2212.11479.
[105] C. Gao, D. Zhao, J. Li, H. Lin, Private bipartite consensus control for multi-agent systems: A hierarchical differential privacy scheme, Inf. Fusion 105 (2024) 102259.
[106] Y. Wang, A. Nedić, Tailoring gradient methods for differentially-private distributed optimization, IEEE Trans. Autom. Control (2023) 1–16.
[107] Z. Huang, S. Mitra, N. Vaidya, Differentially private distributed optimization, in: Proceedings of the 16th International Conference on Distributed Computing and Networking, ICDCN '15, Association for Computing Machinery, New York, NY, USA, 2015, pp. 1–10.
[108] S. Mao, M. Yang, W. Yang, Y. Tang, W.X. Zheng, J. Gu, H. Werner, Differentially private distributed optimization with an event-triggered mechanism, IEEE Trans. Circuits Syst. I. Regul. Pap. 70 (7) (2023) 2943–2956.
[109] E. Nozari, P. Tallapragada, J. Cortés, Differentially private distributed convex optimization via functional perturbation, IEEE Trans. Control Netw. Syst. 5 (1) (2018) 395–408.
[110] J. Zhu, C. Xu, J. Guan, D.O. Wu, Differentially private distributed online algorithms over time-varying directed networks, IEEE Trans. Signal Inf. Process. Netw. 4 (1) (2018) 4–17.
[111] Y. Xiong, J. Xu, K. You, J. Liu, L. Wu, Privacy-preserving distributed online optimization over unbalanced digraphs via subgradient rescaling, IEEE Trans. Control Netw. Syst. 7 (3) (2020) 1366–1378.
[112] Q. Lü, X. Liao, T. Xiang, H. Li, T. Huang, Privacy masking stochastic subgradient-push algorithm for distributed online optimization, IEEE Trans. Cybern. 51 (6) (2021) 3224–3237.
[113] T. Ding, S. Zhu, J. He, C. Chen, X. Guan, Consensus-based distributed optimization in multi-agent systems: Convergence and differential privacy, in: 2018 IEEE Conference on Decision and Control, CDC, IEEE, Miami Beach,FL, USA, 2018, pp. 3409–3414.
[114] T. Ding, S. Zhu, J. He, C. Chen, X. Guan, Differentially private distributed optimization via state and direction perturbation in multiagent systems, IEEE Trans. Autom. Control 67 (2) (2021) 722–737.
[115] T. Zhang, Q. Zhu, Dynamic differential privacy for ADMM-based distributed classification learning, IEEE Trans. Inf. Forensics Secur. 12 (1) (2017) 172–187.
[116] X. Zhang, M.M. Khalili, M. Liu, Improving the privacy and accuracy of ADMM-based distributed algorithms, in: The 35th International Conference on Machine Learning, PMLR, Stockholm, Sweden, 2018, pp. 5796–5805.
[117] X. Zhang, M.M. Khalili, M. Liu, Recycled ADMM: Improving the privacy and accuracy of distributed algorithms, IEEE Trans. Inf. Forensics Secur. 15 (2020) 1723–1734.
[118] R. Dobbe, Y. Pu, J. Zhu, K. Ramchandran, C. Tomlin, Local differential privacy for multi-agent distributed optimal power flow, in: 2020 IEEE PES Innovative Smart Grid Technologies Europe, (ISGT-Europe), IEEE, The Hague, Netherlands, 2020, pp. 265–269.
[119] R. Dobbe, Y. Pu, J. Zhu, K. Ramchandran, C. Tomlin, Customized local differential privacy for multi-agent distributed optimization, 2020, arXiv preprint arXiv:1806.06035.
[120] T. Ding, S. Zhu, C. Chen, J. Xu, X. Guan, Differentially private distributed resource allocation via deviation tracking, IEEE Trans. Signal Inf. Process. Netw. 7 (2021) 222–235.
[121] W. Wu, S. Zhu, S. Liu, X. Guan, Differentially private distributed mismatch tracking algorithm for constraint-coupled resource allocation problems, in: 2022 IEEE 61st Conference on Decision and Control, CDC, Cancún, Mexico, 2022, pp. 3965–3970.
[122] J. Hu, G. Chen, H. Li, T. Huang, L. Ran, Achieving linear convergence for differentially private full-decentralized economic dispatch over directed networks, Inform. Sci. 642 (2023) 119199.
[123] F. Chen, X. Chen, L. Xiang, W. Ren, Distributed economic dispatch via a predictive scheme: Heterogeneous delays and privacy preservation, Automatica 123 (2021) 109356.
[124] Y. Nesterov, Introductory Lectures on Convex Optimization: A Basic Course, vol. 87, Springer Science & Business Media, 2003.
[125] S. Han, U. Topcu, G.J. Pappas, Differentially private distributed constrained optimization, IEEE Trans. Autom. Control 62 (1) (2016) 50–64.
[126] Y. Liu, J. Liu, T. Basar, Differentially private gossip gradient descent, in: 2018 IEEE Conference on Decision and Control, CDC, IEEE, Miami Beach, FL, USA, 2018, pp. 2777–2782.
[127] Y. Yang, X. Guan, Q.-S. Jia, L. Yu, B. Xu, C.J. Spanos, A survey of ADMM variants for distributed optimization: Problems, algorithms and features, 2022, arXiv preprint arXiv:2208.03700.
[128] Z. Liu, F. Guo, W. Wang, X. Wu, A distributed parallel optimization algorithm via alternating direction method of multipliers, IET Control Theory Appl. 17 (7) (2023) 896–905.
[129] T. Zhang, Q. Zhu, Distributed privacy-preserving collaborative intrusion detection systems for VANETs, IEEE Trans. Signal Inf. Process. Netw. 4 (1) (2018) 148–161.
[130] Z. Huang, Y. Gong, Differentially private ADMM for convex distributed learning: Improved accuracy via multi-step approximation, 2020, arXiv preprint arXiv:2005.07890.
[131] C. Gu, L. Jiang, J. Li, Z. Wu, Privacy-preserving dual stochastic push-sum algorithm for distributed constrained optimization, J. Optim. Theory Appl. 197 (1) (2023) 22–50.
[132] L. Yan, X. Chen, Y. Chen, A consensus-based privacy-preserving energy management strategy for microgrids with event-triggered scheme, Int. J. Electr. Power Energy Syst. 141 (2022) 108198.
[133] K. Xu, J. Li, G. Chen, Privacy masking distributed saddle-point algorithm for dynamic economic dispatch, Neural Comput. Appl. 35 (11) (2023) 8109–8123.
[134] D. Zhao, C. Zhang, X. Cao, C. Peng, B. Sun, K. Li, Y. Li, Differential privacy energy management for islanded microgrids with distributed consensus-based ADMM algorithm, IEEE Trans. Control Syst. Technol. 31 (3) (2023) 1018–1031.

Yamin Wang received the B.S. degree in applied mathematics from Southeast University, Nanjing, China, in 2016, and the Ph. D. degree in control engineering from the University of Hong Kong, Hong Kong, in 2022. She is currently a post-doctoral fellow with the Department of Mechanical Engineering, the University of Hong Kong. Her research interests include privacy preservation in networked systems and positive systems.

Hong Lin received the B.S. and M.S. degrees from Fuzhou University, Fuzhou, China, in 2003 and 2006, respectively, and the Ph.D. degree from Zhejiang University, Hangzhou, China, in 2016. He was a lecturer with the Department of Information Technology, Concord College Fujian Normal University, Fuzhou, China, from 2007 to 2012, and was a Postdoctoral Researcher at the Department of Mechanical Engineering, The University of Hong Kong, Hong Kong, from 2016 to 2019.

He is currently with the Institute of Intelligence Science and Engineering, Shenzhen Polytechnic University, Shenzhen, China. His current research interests include networked control systems, estimator design, optimal control, and privacy protection.

James Lam received a B.Sc. (1st Hons.) degree in Mechanical Engineering from the University of Manchester, and was awarded the Ashbury Scholarship, the A.H. Gibson Prize, and the H. Wright Baker Prize for his academic performance. He obtained the MPhil and Ph.D. degrees from the University of Cambridge. He is a Croucher Scholar, Croucher Fellow, and Distinguished Visiting Fellow of the Royal Academy of Engineering, and Cheung Kong Chair Professor. Prior to joining the University of Hong Kong in 1993 where he is now Chair Professor of Control Engineering, he was a faculty member at the City University of Hong Kong and the University of Melbourne.

Professor Lam is a Chartered Mathematician (CMath), Chartered Scientist (CSci), Chartered Engineer (CEng), Fellow of Institute of Electrical and Electronic Engineers (FIEEE), Fellow of Institution of Engineering and Technology (FIET), Fellow of Institute of Mathematics and Its Applications (FIMA), Fellow of Institution of Mechanical Engineers (FIMechE), and Fellow of Hong Kong Institution of Engineers (FHKIE). He is Editor-in-Chief of IET Control Theory and Applications, Journal of The Franklin Institute and Proc. IMechE Part I: Journal of Systems and Control Engineering, Subject Editor of Journal of Sound and Vibration, Editor of Asian Journal of Control, Senior Editor of Cogent Engineering, Section Editor of IET Journal of Engineering, Consulting Editor of International Journal of Systems Science, Associate Editor of Automatica and Multidimensional Systems and Signal Processing. His research interests include model reduction, robust synthesis, delay, singular systems, stochastic systems, multidimensional systems, positive systems, networked control systems and vibration control. He is a Highly Cited Researcher in Engineering (2014, 2015, 2016, 2017, 2018, 2019, 2020) and Computer Science (2015).

Ka-Wai Kwok received the B.Eng. and M.Phil. degrees from Department of Automation and Computer-aided Engineering, The Chinese University of Hong Kong, then obtained the Ph.D. degree from the Hamlyn Centre for Robotic Surgery, Department of Computing, Imperial College London in 2012. Prior to joining The University of Hong Kong (HKU) in 2014, he was awarded the Croucher Foundation Fellowship, which supported his research jointly supervised by advisors in The University of Georgia, and Brigham and Women's Hospital, Harvard Medical School. His research interests focus on surgical robotics, intra-operative image processing, and their uses of intelligent systems. He has participated in various designs of robotic devices/interfaces for endoscopy, and MRI-guided interventions.

Ka-Wai currently serves as Associate Professor at Department of Mechanical Engineering, HKU. To date, he has co-authored >160 peer-reviewed articles with >80 clinical fellows and >160 scientists/engineers. His multidisciplinary work has been recognized by various (>10) awards in international conferences/journals, e.g. the largest flagship conferences of robotics, ICRA and IROS. He was the recipient of ICRA Best Conference Paper Award in 2018, and IROS Toshio Fukuda Young Professional Award in 2020. He also obtained awards in his early career for robotics, e.g. the Early Career Awards 2015/16 offered by Research Grants Council (RGC) of Hong Kong, Actuators 2020 Young Investigator Award, HKU 2019–2020 Outstanding Young Researcher Award, HKU Young Innovator Award 2020 and HKU Research Output Prize 2021–22.

Ka-Wai is the principal investigator of group for Interventional Robotic and Imaging Systems (IRIS) at HKU. The group has (>5) inventions licensed/transferred from university to industry in support for their commercialization. He is a co-founder of Agilis Robotics Ltd. aiming at advancing the interventional endoscopy with small, flexible robotic instruments and their intelligent control systems.