Differential Initial-Value Privacy and Observability of Linear Dynamical Systems

Lei Wang [a], Ian R. Manchester [b], Jochen Trumpf [c], Guodong Shi [b]

[a] *College of Control Science and Engineering, Zhejiang University, China.*

[b] *Australia Centre for Field Robotics, The University of Sydney, Australia.*

[c] *College of Engineering and Computer Science, The Australian National University, Australia.*

Abstract

This paper studies the relationship between the differential privacy of initial values and the observability for general linear dynamical systems with Gaussian process and sensor noises, where certain initial values are privacy-sensitive and the rest is assumed to be public. First of all, necessary and sufficient conditions are established for preserving the differential privacy and unobservability of the global sensitive initial values, respectively to show their independent properties. Specifically, we show that the observability matrix reduced by the set of sensitive initial states not only characterizes the structural property of noises for achieving the differential privacy, but also affects the achievable privacy levels, while the unobservability relies on the rank of such reduced observability matrix. Next, the inherent network nature of the considered linear system is explored, where each individual state corresponds to a node and the state and output matrices induce interaction and sensing graphs, leading to a network system. Under this network perspective, the previously established results are extended for initial values of local nodes to study their differential privacy and connections with their observability. Moreover, it is shown that the qualitative property of the differential initial-value privacy is either *preserved generically* or lost generically, which is the same as the unobservability in the local sense, while subject to a subtle difference from the unobservability in the global sense that is either *preserved fully* or lost generically. Finally, a privacy-preserving consensus algorithm is revisited to illustrate the effectiveness of the established results.

Key words: Initial-value privacy; differential privacy; observability; structural unobservability; average consensus

1 Introduction

The rapid developments in networked control systems [2], internet of things [3, 4], smart grids [5], intelligent transportation [6, 7] during the past decade shed lights on how future infrastructures of our society can be made *smart* via interconnected sensing, dynamics, and control over cyber-physical systems. The operation of such systems inherently relies on users and subsystems sharing signals such as measurements, dynamical states, control inputs in their local views, so that collective decisions become possible. The shared signals might directly contain sensitive information of a private nature, e.g., loads and currents in a grid reflect directly activities in a residence or productions in a company [8]; or they might indirectly encode physical parameters, user preferences, economic inclination, e.g., control inputs in economic model predictive control implicitly carry information about the system's economic objective as it is used as the objective function [9].

Initial values of a dynamical system may carry sensitive private information, leading to privacy risks related to the initial values. For instance, when distributed load shedding in micro-grid systems is performed by employing an average consensus dynamics, initial values represent load demands of individual users [10]. Besides, taking an autonomous vehicle for an instance, the initial position may represent the home address of user [11]. In the literature, several results have been reported to address the initial-value privacy, such as [12–15], where

Email addresses: lei.wangzju@zju.edu.au (Lei Wang), ian.manchester@sydney.edu.au (Ian R. Manchester), Jochen.Trumpf@anu.edu.au (Jochen Trumpf), guodong.shi@sydney.edu.au (Guodong Shi).

[1] *This research is supported by the Australian Research Council Discovery Project DP190103615. A preliminary work has been presented at the 59th IEEE Conference on Decision and Control [1]. The work is done while L. Wang was with Australia Centre for Field Robotics, The University of Sydney, Australia.

the initial-value privacy of the average consensus algorithm over dynamical networks was studied, and injecting noises was used as a privacy-protection approach. The privacy of the initial value for a dynamical system is also of significant theoretical interest as the system trajectories or distributions of the system trajectories are fully parametrized by the initial values, in the presence of the plant knowledge.

Observability is a fundamental notion of dynamical systems, measuring how well the system states can be inferred from measured outputs. This also implies the intrinsic connection between the observability and the initial-value privacy risk. Along this line, the initial-value privacy in the unobservability sense has been studied in [16–18]. Moreover, in [28] a sufficient condition is established, showing that the differential privacy of initial values is also *quantitatively* related to the observability in the sense that the achievable privacy levels rely on the observability matrix. A *qualitative*, and more thorough connection, e.g., from a necessary and sufficient condition, between the differential privacy and the observability is still unclear. Besides, it is worth noting that in the previously mentioned results the whole system initial states are regarded as sensitive. However, in the presence of malicious agents or sensors, or due to the physical nature of certain state entries (e.g. the velocity of an autonomous vehicle), part of the initial states might be subjected to public disclosure. Particularly, though the system initial values or individual initial values can be unobservable from the outputs, they may become observable under such publicly disclosed information, leading to a different observability of initial values. In view of this, it is natural to ask how the observability is related to the differential privacy of initial values in the presence of the disclosed initial values.

In this paper, we consider general linear dynamical systems with Gaussian process and sensor noises, in which there are certain sensitive initial values and the non-sensitive initial values are supposed to be public. For such linear systems, we aim to establish necessary and sufficient conditions so as to comprehensively reveal the fundamental relationship between the differential initial-value privacy and the observability for linear systems.

1.1 Contributions

This paper studies the differential privacy of certain initial values for general linear systems, and explores the connection with the corresponding observability. We first study both concepts from a global level by taking the sensitive initial values as a whole, and then turn to local initial values by exploring the inherent network nature of linear systems, where each dimension of the system state corresponds to a node, and the state and output matrices induce interaction and sensing graphs. The contributions of this paper can be summarized into the following three aspects.

(i) Taking the sensitive initial values as a whole, we establish necessary and sufficient conditions, respectively for both differential privacy and unobservability to show their independent properties. Particularly, both qualitative and quantitative conditions are developed, characterizing the effect of the observability matrix reduced by the sensitive initial states on the noise structure for achieving the differential privacy and the achievable privacy levels by the noises, respectively. In contrast, the unobservability equals to the non-full-rank property of such a reduced observability matrix. This in turn clarifies the fundamentally different roles played by the observability matrix in both notions.

(ii) Taking the system as a networked system, we generalize the results for the global sensitive initial values by establishing necessary and sufficient conditions for the differential privacy and the unobservability of initial values of local nodes, respectively.

(iii) We further investigate the qualitative effect of network structure to differential initial-value privacy, and show that it is either *preserved generically* or lost generically, which is the same as the unobservability in the local sense, while subject to a subtle difference from the unobservability in the global sense which is either *preserved fully* or lost generically.

The structural analysis for differential privacy and unobservability in the presence of disclosed initial values extends the classical work on structural observability [19–21] where generic conditions are established. Besides, the results on differential initial-value privacy may shed insights on privacy preservation of linear systems.

1.2 Related Work

This paper is established on the privacy metrics in the literature to address privacy concerns of dynamical systems. A notable metric is differential privacy, which has received significant attention in the database field since the seminal works [22, 23]. Recently, such privacy metric has been applied to dynamical systems for problems ranging from average consensus seeking [12, 13, 24, 25] and distributed optimization [26, 27] to estimation and filtering [8, 11] and feedback control [28–30]. In particular, random noises are injected to measurements to protect the state-trajectory privacy, with initial-value privacy as a particular case, for a filtering problem in [11] and a cloud-based linear quadratic regulation problem in [29]. In [28], the differential privacy of control inputs and initial states is investigated for linear control systems. It is shown that the (input) observability affects the differential privacy levels that can be achieved by the added noises. In [13], an average consensus algorithm is developed by perturbing the communication messages and computation procedures with exponentially decaying noises to preserve the differential privacy of initial

values, and an optimal policy has been established by perturbing the initial values with random noises. We note that all these results consider a strong differential privacy requirement in the sense that there is no public information on the privacy-sensitive data, which is different from our case where there are some public initial values. Moreover, this paper also develops qualitative conditions on the noise structure and studies the generic property of the differential privacy, which are absent in these results.

Another related but different privacy risk lies in the possibility of making an accurate enough estimation of the sensitive parameters or signals from observations. In [17,18], the initial-value privacy is defined in the sense that the initial values cannot be deterministically recovered. In [16] the variance matrix of the maximum likelihood estimation was utilized to measure the adversary's inherent ability to infer system states, with initial states as a particular case. If the system is unobservable from the adversary's observations, then the resulting variance matrix is not finite, leading to the so-called security of the system states. This idea is further developed in [15] to propose a privacy-preserving average consensus with a malicious node. In [31], a measure of privacy was developed using the inverse of the trace of the Fisher information matrix, which is a lower bound of the variance of estimation error of unbiased estimators.

The study of unobservability of initial values and its generic property in this paper are of relevance to the works on the classical observability/controllability and their structural properties [21], respectively. Recent advances along these lines contain such as [32] for structural controllability of symmetric networks, [33] for structural observability of bilinear systems, [34] for structural state variable controllability and [35,36] for strong structural controllability. Readers of interest can see [20] for a survey. It is worth noting that the notion of observability has been developed for undetectable attacks in [37,38]. Compared to these relevant results, our (generic) unobservability of global sensitive initial values can be regarded as a generalization of the classical (structural) unobservability by additionally considering the effect of the public non-sensitive initial values. Besides, the unobservability of local initial values is shown to be either *preserved generically* or *lost generically*, which is indeed different from the classical structural properties [20,21,32,33], in which the observability/controllability is either *generically preserved* or *fully lost*.

1.3 Organization and Notation

The remainder of the paper is organized as follows. Section 2 formulates the problem of interest for linear (networked) systems. In Section 3, the relationship between the differential privacy and unobservability of sensitive initial values as a whole is addressed. Then regarding the system from the network perspective, the previously established results are extended to study differential initial-value privacy of local nodes and its connection with the observability in Section 4, and in Section 5 the generic properties of all these differential privacy and unobservability are discussed from a qualitative perspective. To illustrate the effectiveness of the proposed results, the privacy-preserving average consensus algorithm proposed in [15] is revisited in Section 6. Finally a brief conclusion is made in Section 7. All technical proofs are presented in Appendices. This paper is a significant extension over the preliminary version [1] by developing new technical results in Theorems 1-4 and illustrative examples.

Notation. Denote by $\mathbb{R}$ the real numbers, $\mathbb{R}^n$ the real space of n dimension for any positive integer n and $\mathbb{N}$ the set of natural numbers. For any $x_1,\dots,x_m\in\mathbb{R}^n$, we denote $[x_1;\dots;x_m]$ as a vector $\begin{bmatrix}x_1^\top & \dots & x_m^\top\end{bmatrix}^\top\in\mathbb{R}^{mn}$, and $[x_1,\dots,x_m]$ as a matrix of which the i-the column is x_i, $i=1,\dots,m$. For any matrix $A\in\mathbb{R}^{n\times m}$, denote $A^\dagger$ as its Moore–Penrose inverse. The range of a matrix (i.e., column space) or a function is denoted as range$(\cdot)$, and the span of a matrix (i.e., row space) is denoted as span$(\cdot)$. Denote $\mathbf{e}_i\in\mathbb{R}^n$ as a basis vector whose entries are all zero except the i-th being one. For any set $\mathrm{P}\subseteq\{1,2,\dots,n\}$ of l elements, we denote $\mathbf{E}_{\mathrm{P}}\in\mathbb{R}^{n\times l}$ as the matrix with each column as a basis vector $\mathbf{e}_j$ with $j\in\mathrm{P}$. We denote by $\boldsymbol{\eta}\sim\mathcal{N}(0,\Sigma)$ if $\boldsymbol{\eta}$ is drawn from a multivariate Gaussian distribution with zero mean and covariance matrix Σ. Given a symmetric, positive (semi)-definite matrix $\Sigma\in\mathbb{R}^{n\times n}$, we denote $\sqrt{\Sigma}$ as a matrix $A\in\mathbb{R}^{n\times n}$ satisfying $A^\top A=\Sigma$.

2 Problem Statement

2.1 Preliminaries

We consider the following linear time-invariant (LTI) system

$$\begin{aligned}\mathbf{x}_{t+1} &= \mathbf{A}\,\mathbf{x}_t+\boldsymbol{\nu}_t\\ \mathbf{y}_t &= \mathbf{C}\,\mathbf{x}_t+\boldsymbol{\omega}_t\end{aligned}\tag{1}$$

for $t\in\mathbb{N}$, where $\mathbf{x}_t:=[x_{1,t};\dots;x_{n,t}]\in\mathbb{R}^n$ is state, $\mathbf{y}_t\in\mathbb{R}^m$ is output, $\boldsymbol{\nu}_t\in\mathbb{R}^n$ is process noise, and $\boldsymbol{\omega}_t\in\mathbb{R}^m$ is measurement noise. Throughout the paper, we assume that $\boldsymbol{\nu}_t$ and $\boldsymbol{\omega}_t$ are random variables according to some zero-mean multivariate Gaussian distributions, but not necessary to be mutually independent, and $\mathbf{C}\neq 0$.

In this paper, we let certain initial values $\mathbf{x}_0^{\mathrm{P}}:=\mathbf{E}_{\mathrm{P}}^\top\mathbf{x}_0$ of system (1) be privacy-sensitive, with $\mathrm{P}\subseteq\mathrm{V}:=\{1,\dots,n\}$, and denote the rest initial states as $\mathbf{x}_0^{\mathrm{D}}=\mathbf{E}_{\mathrm{D}}^\top\mathbf{x}_0$ with $\mathrm{D}=\mathrm{V}/\mathrm{P}$. Besides, we impose the following assumption.

Assumption 1 *The system matrices* $\mathbf{A}, \mathbf{C}$*, the initial states* $\mathbf{x}_0^{\mathrm{D}}$ *and the output* $\mathbf{y}_t$ *for* $t = 0, 1, \ldots, T$ *are public.*

It is known that if the system (1) is observable, then the system initial values $\mathbf{x}_0$ are identifiable/observable (or accurately estimated in the absence of noises) from the output. This clearly implies the intrinsic connection between the initial-value exposure risk and the observability of linear systems. In view of this, this paper aims to further study the connection of the observability with the initial-value privacy, with a particular focus on an increasingly popular notion of differential privacy [39], as defined in the subsequent subsections. As a result, this can not only add to our understanding of initial-value privacy for linear systems, but also provide insights on the role of the observability in protecting differential privacy of initial states.

It is worth noting that this paper considers a general scenario where certain initial values $\mathbf{x}_0^{\mathrm{P}}$ are privacy-sensitive, with the overall initial values $\mathbf{x}_0$ being sensitive, i.e., $\mathrm{P} = \mathrm{V}$ as a particular case. This is mainly because each system state may have a different physical meaning and only a part of their initial values contain sensitive information. For example, consider dynamical systems of autonomous vehicles [11], in which initial positions may be sensitive as they may represent private information (e.g. home addresses) of users, while initial velocities are not sensitive. Besides, in Assumption 1 the non-privacy-sensitive initial states $\mathbf{x}_0^{\mathrm{D}}$ are assumed to be disclosed, which, on the one hand allows the considered setup applicable to more general adversaries, and on the other hand, is motivated from practical scenarios. For example, the vehicle from home has a public initial velocity as zero. Besides, when running a consensus algorithm to compute the average of initial values (i.e., loads) for the load shedding problem in a power grid [10], some of the network initial values are public, e.g., since they belong to government organizations that openly publish their energy usage, while the remainder belongs to private users and their energy usage is considered commercially sensitive. In view of the different properties of the initial values associated to the sets P and D, we thus term the sets P and D as the *private set* and the *disclosed set*, respectively in the sequel.

Remark 1 *It is noted that the noises* $\boldsymbol{\nu}_t$ *and* $\boldsymbol{\omega}_t$ *in the system (1) may also contain the noises injected for privacy protection, such as the noises added to the measured positions in a privacy-preserving traffic monitoring system [11], or the noises added to both the iteration process and communication messages in the privacy-preserving average consensus algorithm [13, 15].*

2.2 Global Initial-Value Privacy

In this subsection, we take the sensitive initial values $\mathbf{x}_0^{\mathrm{P}}$ as a whole and specify the differential privacy and the unobservability of $\mathbf{x}_0^{\mathrm{P}}$ for the system (1), respectively.

To facilitate the subsequent definitions, we denote the measurement vector $\mathbf{Y}_T = [\mathbf{y}_0; \mathbf{y}_1; \ldots; \mathbf{y}_T]$, the noise vectors $\mathbf{V}_T = [\boldsymbol{\nu}_0; \boldsymbol{\nu}_1; \ldots; \boldsymbol{\nu}_{T-1}]$ and $\mathbf{W}_T = [\boldsymbol{\omega}_0; \boldsymbol{\omega}_1; \ldots; \boldsymbol{\omega}_T]$, and

$$\mathbf{O}_t = \begin{bmatrix} \mathbf{C} \\ \mathbf{CA} \\ \vdots \\ \mathbf{CA}^t \end{bmatrix}, \ \mathbf{H}_t = \begin{bmatrix} 0 & 0 & \cdots & 0 & 0 \\ \mathbf{C} & 0 & \ddots & 0 & 0 \\ \mathbf{CA} & \mathbf{C} & \ddots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \mathbf{CA}^{t-2} & \mathbf{CA}^{t-3} & \ddots & \mathbf{C} & 0 \\ \mathbf{CA}^{t-1} & \mathbf{CA}^{t-2} & \cdots & \mathbf{CA} & \mathbf{C} \end{bmatrix}.$$

Thus, the mapping from the initial state $\mathbf{x}_0$ to the output trajectory $\mathbf{Y}_T$ as $\mathscr{M} : \mathbb{R}^n \to \mathbb{R}^{m(T+1)}$ can be described by

$$\mathbf{Y}_T = \mathscr{M}(\mathbf{x}_0) := \mathbf{O}_T \mathbf{x}_0 + \mathbf{H}_T \mathbf{V}_T + \mathbf{W}_T \,. \tag{2}$$

Then we introduce the following definitions.

Definition 1 *Let the private set* $\mathrm{P} \subseteq \mathrm{V}$ *and the disclosed set* $\mathrm{D} = \mathrm{V} \backslash \mathrm{P}$*.*

(a) The initial values $\mathbf{x}_0^{\mathrm{P}}$ *of system (1) are* (ϵ, δ)-differentially private *under* μ*-adjacency for* $\epsilon \geq 0$*,* $\delta \in [0, 1)$ *and* $\mu > 0$*, if for all* $\mathcal{M} \subseteq$ *range*$(\mathscr{M})$*,*

$$\mathbb{P}(\mathscr{M}(\mathbf{x}_0) \in \mathcal{M}) \leq e^{\epsilon}\, \mathbb{P}(\mathscr{M}(\hat{\mathbf{x}}_0) \in \mathcal{M}) + \delta \tag{3}$$

for any $\mathbf{x}_0, \hat{\mathbf{x}}_0 \in \mathbb{R}^n$*, satisfying* $\mathbf{x}_0^{\mathrm{D}} = \hat{\mathbf{x}}_0^{\mathrm{D}}$ *and* $\|\mathbf{x}_0^{\mathrm{P}} - \hat{\mathbf{x}}_0^{\mathrm{P}}\| \leq \mu$*.*

(b) The initial values $\mathbf{x}_0^{\mathrm{P}}$ *of system (1) are* unobservable*, if for any initial state* $\mathbf{x}_0 \in \mathbb{R}^n$*, there exists* $\hat{\mathbf{x}}_0 \in \mathbb{R}^n$ *satisfying* $\mathbf{x}_0^{\mathrm{D}} = \hat{\mathbf{x}}_0^{\mathrm{D}}$ *and* $\mathbf{x}_0^{\mathrm{P}} \neq \hat{\mathbf{x}}_0^{\mathrm{P}}$*, such that for all* $\mathcal{M} \subseteq$ *range*$(\mathscr{M})$*,*

$$\mathbb{P}(\mathscr{M}(\mathbf{x}_0) \in \mathcal{M}) = \mathbb{P}(\mathscr{M}(\hat{\mathbf{x}}_0) \in \mathcal{M}) \,. \tag{4}$$

The notion of differential initial-value privacy in Definition 1.(a) follows the standard differential privacy [23, 39] and has been studied in [13,30]. Particularly, under a particular case with an empty D, it is shown in [30] that the achievable differential privacy levels (ϵ, δ, μ) rely on the observability matrix $\mathbf{O}_T$. The notion of unobservability in Definition 1.(b) can be regarded as a simple generalization of the standard unobservability of the system (1) in the presence of the noises and the disclosed set. From a conceptual perspective, the $\hat{\mathbf{x}}_0$ satisfying (4) yields (3) with $\epsilon = \delta = 0$. However we cannot say that the unobservability of $\mathbf{x}_0^{\mathrm{P}}$ implies its $(0, 0)$-differential privacy, as there is no guarantee that such $\hat{\mathbf{x}}_0$ can be arbitrary in the μ-adjacency of $\mathbf{x}_0$. On the other hand, it is clear that when $\epsilon = \delta = 0$, the (ϵ, δ)-differential privacy of $\mathbf{x}_0^{\mathrm{P}}$ implies its unobservability, while for other cases of (ϵ, δ), there is no guarantee of such implication.

Remark 2 *In this paper, we focus on the additive noises* $\boldsymbol{\nu}_t, \boldsymbol{\omega}_t$ *in* (1) *according to Gaussian distributions, which renders the mapping* $\mathscr{M}$ *in* (2) *to be a Gaussian mechanism and makes the subsequent privacy analysis convenient. However, considering that these noises may be designed for preserving initial-value privacy as addressed in Remark 1, it is worth noting that they may be multiplicative noises [43] or additive Laplace noises [13] for other type of mechanisms, under which the desired differential privacy can be preserved, but with possibly new noise requirements compared to the conditions given in the forthcoming Theorems 1 and 2.*

2.3 Linear Networked Systems and Local Initial-Value Privacy

The system (1) can also be understood from a network system perspective, e.g., [41]. Let $x_{i,t}$ be the i-th entry of $\mathbf{x}_t$. By viewing each $x_{i,t}$ as the dynamical state of a node, the matrix $\mathbf{A}$ indicates a graph of interactions among the nodes. Similarly, viewing each entry of $\mathbf{y}_t$ as the measurement of a sensor, the matrix $\mathbf{C}$ indicates a graph of interactions between the nodes and the sensors. In this respect, we consider a network consisting of n network nodes and m sensing nodes, leading to a network node set $\mathrm{V} = \{1, \ldots, n\}$ and a sensing node set $\mathrm{V_S} = \{s_1, \ldots, s_m\}$ [2], respectively. Define the interaction graph $\mathrm{G} = (\mathrm{V}, \mathrm{E})$ with edge set $\mathrm{E} \subset \mathrm{V} \times \mathrm{V}$, and the sensing graph $\mathrm{G_S} = (\mathrm{V}, \mathrm{V_S}, \mathrm{E_S})$ with edge set $\mathrm{E_S} \subset \mathrm{V} \times \mathrm{V_S}$. Then, the private set P represents a set of nodes whose initial states are confidential, while the disclosed set D represents the rest nodes whose initial states are non-confidential and public. Let $\mathbf{A} = [a_{ij}] \in \mathbb{R}^{n\times n}$ and $\mathbf{C} = [c_{ij}] \in \mathbb{R}^{m\times n}$. We say $(\mathbf{A}, \mathbf{C})$ to be a configuration complying with the graphs $\mathrm{G}, \mathrm{G_S}$, if $a_{ij} = 0$ for $(j, i) \notin \mathrm{E}$ and $c_{ij} = 0$ for $(j, s_i) \notin \mathrm{E_S}$.

In the network setting, the local agent is concerned about its own local initial-value privacy. In the following, we generalize the global notions in Definition 1 to the network setting for local privacy and unobservability.

Definition 2 *Given any network structure* $\mathrm{G}, \mathrm{G_S}$*, let the private set* $\mathrm{P} \subseteq \mathrm{V}$*, the disclosed set* $\mathrm{D} = \mathrm{V}\backslash\mathrm{P}$ *and* $(\mathbf{A}, \mathbf{C})$ *be any configuration complying with graphs* $\mathrm{G}, \mathrm{G_S}$*.*

(a) The initial-value of node $i \in \mathrm{P}$ *is* (ϵ, δ)-differentially private *under* μ*-adjacency for* $\epsilon \geq 0$*,* $\delta \in [0, 1)$ *and* $\mu > 0$*, if for all* $\mathcal{M} \subseteq$ *range*$(\mathscr{M})$*, (3) holds for any non-identical* $\mathbf{x}_0, \hat{\mathbf{x}}_0 \in \mathbb{R}_n$*, satisfying* $|x_{i,0} - \hat{x}_{i,0}| \leq \mu$ *and* $x_{j,0} = \hat{x}_{j,0}$ *for all* $j \neq i$*.*

(b) The initial-value of node $i \in \mathrm{P}$ *is* unobservable*, if for any initial state* $\mathbf{x}_0 \in \mathbb{R}^n$*, there exists* $\hat{\mathbf{x}}_0 \in \mathbb{R}^n$ *such that* $x_{i,0} \neq \hat{x}_{i,0}$*,* $x_{j,0} = \hat{x}_{j,0}$ *for* $j \in \mathrm{D}$*, and (4) holds.*

[2] To be distinguished with notations for nodes in the interaction graph G, we use s_i to denote the i-th sensing node whose measurement is y_i.

Under a particular case with $\mathrm{P} = \mathrm{V}$, we note that the unobservability of node i's initial value is equivalent to state variable unobservability of the node state $x_{i,t}$, a dual notion of state variable uncontrollability [34].

Remark 3 *In Definition 2.(a), the pair* $(\mathbf{x}_0, \hat{\mathbf{x}}_0)$ *is required to be distinct only at the* i*-th entry, which differs from the global version in Definition 1.(a). The intuition behind such difference lies in establishing a strong local initial-value privacy in the sense that even if all initial values of other nodes are known to an adversary, it should still be difficult for the adversary to infer the initial value of node* i*, measured by* (ϵ, δ, μ)*. In Definition 2.(b), the pair* $(\mathbf{x}_0, \hat{\mathbf{x}}_0)$ *is required to be distinct at the* i*-th entry and same at the entries in the disclosed set* D*, while having no requirement to the nodes in* $\mathrm{V}\backslash\{\mathrm{D} \cup \{i\}\}$*, as node* i *is concerned about only its own local initial value.*

2.4 Problems of Interest

In this paper, we will focus on the differential privacy and unobservability of certain initial values $\mathbf{x}_0^{\mathrm{P}}$ for system (1), from both global and local perspectives, and explore the effect of network structure to these notions. To be precise, we aim to investigate the following questions:

(Q1) From a global perspective, when will the differential privacy and unobservability of $\mathbf{x}_0^{\mathrm{P}}$ be preserved, and in particular, what is the relationship between both notions?

(Q2) If we zoom in the study and focus on the local initial value for a node $i \in \mathrm{P}$, what will be the conditions of the differential privacy and unobservability?

(Q3) How the structure of the interaction and sensing graphs affects the privacy preservation conditions and the unobservability conditions, respectively?

Answers to these questions (detailed in the subsequent three sections, respectively) will add to our understanding of differential initial-value privacy for linear systems, the role of the observability in preserving the differential initial-value privacy of linear systems, and also the effect of the network structure to the differential initial-value privacy for a linear network system.

3 Global Initial-Value Privacy of Linear Systems

3.1 Global Differential Initial-Value Privacy and Unobservability

Let $(\mathbf{V}_T; \mathbf{W}_T) \backsim \mathcal{N}(0, \Sigma_T \Sigma_T^\top)$ and matrix $\Omega_T = [\mathbf{H}_T \ \ \mathbf{I}_{m(T+1)}]\Sigma_T$, and denote

$$\Delta_{\mathrm{P}} := \|\sqrt{(\Omega_T \Omega_T^\top)^\dagger}\mathbf{O}_T \mathbf{E}_{\mathrm{P}}\|, \tag{5}$$

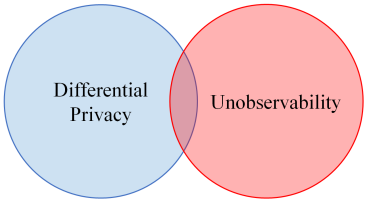

Figure 1. Relationship between the differential privacy and the unobservability of initial values.

and the *extended* observability matrix by the disclosed set D as $\mathbf{O}_T^{\mathrm{D}} := [\mathbf{O}_T;\ \mathbf{E}_{\mathrm{D}}^\top]$. We then introduce function

$$\kappa(r,s) := \mathcal{Q}(\frac{s}{2}-\frac{r}{s}) - e^r\mathcal{Q}(-\frac{s}{2}-\frac{r}{s}) \tag{6}$$

with $\mathcal{Q}(w) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{w} e^{-\frac{v^2}{2}}dv$. It is noted that

$$\frac{\partial\kappa(r,s)}{\partial s} = \frac{1}{\sqrt{2\pi}}\exp\Big(-\frac{1}{2}(\frac{s}{2}-\frac{r}{s})^2\Big) > 0\,,$$

which implies that $\kappa(r,s)$ is a strictly increasing function with respect to $s>0$, uniformly in r. For convenience, given any r, we denote by $\kappa_r^{-1}(\cdot)$ the inverse of the function $\kappa(r,s)$ with respect to s.

The following results establish necessary and sufficient conditions for both the differential privacy and unobservability of initial values $\mathbf{x}_0^{\mathrm{P}}$, demonstrating that both notions are mutually independent (see Fig. 1).

Theorem 1 *Let Assumption 1 hold. The differential privacy and unobservability of initial values $\mathbf{x}_0^{\mathrm{P}}$ for system (1) are independent properties.*

(i). The initial values $\mathbf{x}_0^{\mathrm{P}}$ of system (1) is (ϵ,δ)-differentially private under μ-adjacency for $\epsilon\geq 0$, $\delta\in(0,1)$ and $\mu>0$, if and only if *there hold the following both conditions*

$$\text{rank}\ (\Omega_T) = \text{rank}\ ([\Omega_T\ \mathbf{O}_T\mathbf{E}_{\mathrm{P}}])\,, \tag{7}$$

$$\Delta_{\mathrm{P}} \leq \kappa_\epsilon^{-1}(\delta)/\mu\,. \tag{8}$$

(ii). The initial values $\mathbf{x}_0^{\mathrm{P}}$ of system (1) is unobservable if and only if

$$\text{rank}\ \big(\mathbf{O}_T^{\mathrm{D}}\big) < n\,. \tag{9}$$

The key ideas in the proof of Theorem 1.(i) and (ii) lie in transforming the differential privacy of $\mathscr{M}$ in (2) to the problem considered in [40] and constructing the $\hat{\mathbf{x}}_0$ in Definition 1.(ii), respectively.

Theorem 1.(i) implies that the necessary and sufficient conditions for the (ϵ,δ)-differential privacy are comprised of two ingredients: (7) and (8), playing different roles in achieving the (ϵ,δ)-differential privacy of $\mathbf{x}_0^{\mathrm{P}}$. Specifically, the former indicates that the column subspace of the P-reduced observability matrix $\mathbf{O}_T\mathbf{E}_{\mathrm{P}}$ is contained by that of Ω_T, characterizing the structural property of the noise covariance $\Sigma_T\Sigma_T^\top$ for the differential privacy, while the latter quantifies the privacy levels that can be achieved by the amount of noises. It is worth noting that given any structured noise covariance $\Sigma_T\Sigma_T^\top$ satisfying the *qualitative* condition (7), there always exists a finite privacy budget $\epsilon\geq 0$ such that the *quantitative* condition (8) is satisfied under any fixed $0<\delta<1$ and $\mu>0$. In view of this, it can be easily verified that if and only if (7) holds, the differential privacy of $\mathbf{x}_0^{\mathrm{P}}$ is preserved with a finite privacy budget $\epsilon\geq 0$ for any $0<\delta<1$ and $\mu>0$, which implies a *qualitative* property of the differential privacy of $\mathbf{x}_0^{\mathrm{P}}$ and is termed *the differential privacy of initial values $\mathbf{x}_0^{\mathrm{P}}$ with a finite privacy budget* in the sequel.

In Theorem 1.(ii), (9) indicates that the D-*extended* observable subspace, denoted by span $\big(\mathbf{O}_T^{\mathrm{D}}\big)$, does not span the whole state space. We notice that

$$\text{rank}\ \big(\mathbf{O}_T^{\mathrm{D}}\big) = \text{rank}\ \big(\mathbf{O}_T^{\mathrm{D}}[\mathbf{E}_{\mathrm{P}}\ \mathbf{E}_{\mathrm{D}}]\big) = \text{rank}\ (\mathbf{O}_T\mathbf{E}_{\mathrm{P}}) + |\mathrm{D}|$$

which, together with (9), implies that the rank of $\mathbf{O}_T\mathbf{E}_{\mathrm{P}}$ determines the unobservability of $\mathbf{x}_0^{\mathrm{P}}$. In contrast, from (7) the effective randomness structure (i.e., the structure of Σ_T) for the differential privacy of $\mathbf{x}_0^{\mathrm{P}}$ relies on the column subspace of $\mathbf{O}_T\mathbf{E}_{\mathrm{P}}$, which characterizes the minimum feasible column subspace of Ω_T. Besides, by (8) and (5) the $\mathbf{O}_T\mathbf{E}_{\mathrm{P}}$ also affects the privacy levels that can be achieved. Thus, the P-reduced observability matrix $\mathbf{O}_T\mathbf{E}_{\mathrm{P}}$ affects the differential privacy of $\mathbf{x}_0^{\mathrm{P}}$ in both qualitative and quantitative senses. This, in turn, demonstrates the difference between the differential privacy and unobservability of $\mathbf{x}_0^{\mathrm{P}}$ in terms of the P-reduced observability matrix $\mathbf{O}_T\mathbf{E}_{\mathrm{P}}$.

Remark 4 *In [28, Theorem 2.6], a sufficient condition similar to (8) is proposed to quantify the achievable privacy levels for linear systems with control inputs by applying the computation method in [11], which is different from the one used in the paper based on [40, Theorem 5] from the perspective of privacy loss. As a result, this leads to a more general quantifiable condition, rendering a necessary and sufficient condition, and a more general range of privacy levels ($\epsilon\geq 0, 0<\delta<1$) in contrast with the condition $\epsilon>0$ and $0<\delta<1/2$ established in [11, 28]. As for the qualitative condition, we note that Ω_T is assumed to be full-rank in [28], which enables (7) satisfied automatically.*

Remark 5 *We remark that the effect of the disclosed set* D *on the differential privacy and unobservability of initial values $\mathbf{x}_0^{\mathrm{P}}$ is different. By increasing the number of entries in* D*, the column subspace of the resulting* P*-reduced observability matrix $\mathbf{O}_T\mathbf{E}_{\mathrm{P}}$ becomes tightened, rendering a* less restrictive qualitative condition *(7) in terms*

of Ω_T and thus the noise structure, while the $\Delta_{\rm P}$ defined in (5) reduces, leading to a larger requirement of μ with fixed (ϵ,δ) by (8), i.e., a stronger differential privacy. *In contrast, the dimension of the* D*-extended observable subspace* span $\left(\mathbf{O}_T^{\rm D}\right)$ *increases as the* D *is enlarged, implying a* weaker unobservability *in the sense that more information on the initial values is observable.*

Remark 6 *If the noises $\boldsymbol{\nu}_t, \boldsymbol{\omega}_t$ (i.e., the covariance $\Sigma_T^\top \Sigma_T$) are design freedoms for (ϵ,δ)-differential initial-value privacy with μ-adjacency, Theorem 1.(i) indeed implies a two-step design method as below.*

(1) Fix a matrix $\bar{\Sigma}_T \in \mathbb{R}^{m(2T+1)\times h}$ for some $h \in \mathbb{N}$, e.g., $[\mathbf{0}_{mT}; \mathbf{I}_{m(T+1)}]$, such that

$$\text{rank}\,(\bar{\Omega}_T) = \text{rank}\,([\bar{\Omega}_T\ \mathbf{O}_T\mathbf{E}_{\rm P}]) = h$$

with $\bar{\Omega}_T := [\mathbf{H}_T\ \ \mathbf{I}_{m(T+1)}]\bar{\Sigma}_T$.

(2) Design $\Sigma_T = \bar{\Sigma}_T\Lambda$ with $\Lambda \in \mathbb{R}^{h\times h}$ being an invertible matrix such that

$$\|\Lambda^{-1}\bar{\Omega}_T^\dagger \mathbf{O}_T\mathbf{E}_{\rm P}\| \leq \kappa_\epsilon^{-1}(\delta)/\mu\,.$$

It is noted that due to the presence of the structural constraint (7), an optimal design of Σ_T, e.g., in the sense of minimizing the trace of the noise covariance $\Sigma_T\Sigma_T^\top$ as in [44], turns out a non-trivial optimization problem, which is out of the scope of this paper and needs to be further studied in the future.

3.2 An Illustrative Example

In this subsection, an illustrative example is presented to demonstrate the relationship between the differential privacy and the unobservability.

Example 1. Consider system (1) with

$$\mathbf{A} = \begin{bmatrix} 1 & 3 \\ 1 & -1 \end{bmatrix}, \mathbf{C} = \begin{bmatrix} 1 & 1 \end{bmatrix}, \boldsymbol{\nu}_t = 0\,, \boldsymbol{\omega}_t \backsim \mathcal{N}(0, \sigma_t^2)$$

and let $T = 2$, which yields

$$\begin{bmatrix} \mathbf{y}_0 \\ \mathbf{y}_1 \\ \mathbf{y}_2 \end{bmatrix} = \mathscr{M}(\mathbf{x}_0) := \mathbf{O}_T\mathbf{x}_0 + \mathbf{W}_T\,, \quad \mathbf{O}_T = \begin{bmatrix} 1 & 1 \\ 2 & 2 \\ 4 & 4 \end{bmatrix}.$$

Regarding the differential initial-value privacy, we let the noises $\boldsymbol{\omega}_t$, $t = 0, 1, 2$ be i.i.d., and observe that $\Omega_T = \text{diag}(\sigma_0, \sigma_1, \sigma_2)$.

- For $\sigma_0 = 0$ and $\sigma_1, \sigma_2 > 0$, as rank (Ω_T) = 2 and rank $([\Omega_T\,\mathbf{O}_T])$ = 3, we have rank $(\Omega_T) \neq$ rank $([\Omega_T\ \mathbf{O}_T\mathbf{E}_{\rm P}])$ for all ${\rm P} \subseteq \{1,2\}\backslash\emptyset$, indicating that the differential privacy of initial values $\mathbf{x}_0^{\rm P}$ cannot be achieved by Theorem 1.(i).
- For $\sigma_0, \sigma_1, \sigma_2 > 0$, we can obtain rank $(\Omega_T) = 3$. Thus, the condition (7) is satisfied with any ${\rm P} \subseteq \{1,2\}\backslash\emptyset$. It is noted that rank $(\mathbf{O}_T) = 1$, which indicates that the noises ω_t satisfying (7) are not necessarily i.i.d. but can be correlated, e.g., $\boldsymbol{\omega}_2 = 2\boldsymbol{\omega}_1 = 4\boldsymbol{\omega}_0$. Regarding the condition (8), we let $\sigma_t = 1$ and choose $\mu = 1$, and by the guideline in [39] that δ is less than any inverse of polynomials in the size of the database, let $\delta = 10^{-2}$. It then can be computed from (8) that the mapping $\mathscr{M}(\mathbf{x}_0)$ is (ϵ,δ)-differentially private with $\epsilon = 36.0768$ for ${\rm P} = \{1,2\}$ and $\epsilon = 21.1609$ for ${\rm P} = \{1\}$ and ${\rm P} = \{2\}$.

For the unobservability, we have the following.

- For ${\rm P} = \{1,2\}$, $\mathbf{x}_0^{\rm P}$ is unobservable for $\sigma_t \geq 0$, $t = 0, 1, 2$ by Theorem 1.(ii) as rank $(\mathbf{O}_T^{\rm D}) = 1 < 2$.
- For either ${\rm P} = \{1\}$ or ${\rm P} = \{2\}$, $\mathbf{x}_0^{\rm P}$ turns out observable for $\sigma_t \geq 0$, $t = 0, 1, 2$ by Theorem 1.(ii) as rank $(\mathbf{O}_T^{\rm D}) = 2$.

In view of the above analysis, both notions of differential privacy and unobservability of initial values in Definition 1 are neither inclusive nor exclusive, validating Theorem 1.

4 Local Initial-Value Privacy of Linear Networked Systems

In this section, we regard (1) as a networked system as specified in Section 2.3 and study the local differential initial-value privacy and local unobservability following Definition 2.

Define $\Delta_i := \|\sqrt{(\Omega_T\Omega_T^\top)^\dagger}\mathbf{O}_T\mathbf{e}_i\|$. We present the following result.

Theorem 2 *Take $i \in {\rm P} \subseteq {\rm V}$ and let Assumption 1 hold.*

(i) The (ϵ,δ)-differential initial-value privacy of node i under μ-adjacency is preserved for $\epsilon \geq 0$, $\delta \in (0,1)$ and $\mu > 0$, if and only if there hold the following both conditions

$$\text{rank}\,(\Omega_T) = \text{rank}\,\left(\begin{bmatrix}\Omega_T\ \ \mathbf{O}_T\mathbf{e}_i\end{bmatrix}\right), \tag{10}$$

$$\Delta_i \leq \kappa_\epsilon^{-1}(\delta)/\mu\,. \tag{11}$$

(ii) The initial value of node i is unobservable if and only if

$$\text{rank}\,\left(\begin{bmatrix}\mathbf{O}_T^{\rm D} \\ \mathbf{e}_i^\top\end{bmatrix}\right) = \text{rank}\,\left(\mathbf{O}_T^{\rm D}\right) + 1\,. \tag{12}$$

From (10) and (11) it can be seen that the i-th column of the observability matrix, i.e., $\mathbf{O}_T\mathbf{e}_i$ affects the local differential initial-value privacy of node i qualitatively and quantitatively. In contrast, Theorem 2.(ii) demonstrates that the unobservability of $x_{i,0}$ is preserved if and only if $\mathbf{e}_i$ does not belong to the D-*extended* observable subspace span $\left(\mathbf{O}_T^{\mathrm{D}}\right)$. This thus implies the mutually independent relationship between the differential privacy and the unobservability of local initial value $x_{i,0}$. Similar to the discussions after Theorem 1, it is seen that if and only if (10) holds, the differential privacy of node i is preserved with a finite privacy budget $\epsilon \geq 0$, for any $0 < \delta < 1$ and $\mu > 0$, which also implies a qualitative property of the local differential privacy in Definition 2.(i), termed the differential initial-value privacy of node i with a finite privacy budget in the sequel.

Remark 7 *We observe that*

$$\begin{aligned}&\text{rank } \left(\mathbf{O}_T^{\mathrm{D}}\right) = \text{rank } \left(\mathbf{O}_T\mathbf{E}_{\bar{\mathrm{P}}}\right) + |\mathrm{D}|\\ &\text{rank } \left(\begin{bmatrix}\mathbf{O}_T^{\mathrm{D}}\\ \mathbf{e}_i^\top\end{bmatrix}\right) = \text{rank } \left(\begin{bmatrix}\mathbf{O}_T\\ \mathbf{e}_i^\top\end{bmatrix}\mathbf{E}_{\mathrm{P}}\right) + |\mathrm{D}|\,.\end{aligned}$$

Thus, (12) can be simplified as

$$\text{rank } \left(\begin{bmatrix}\mathbf{O}_T\\ \mathbf{e}_i^\top\end{bmatrix}\mathbf{E}_{\mathrm{P}}\right) = \text{rank } \left(\mathbf{O}_T\mathbf{E}_{\mathrm{P}}\right) + 1\,. \tag{13}$$

In view of this, we occasionally use (13) to replace (12) in Theorem 2.(ii) in the sequel.

Remark 8 *It is noted that the row subspace of $\mathbf{O}_t$ does not change as $t \geq n-1$ increases. Namely, by letting $\mathbf{O}_{ob} = \mathbf{O}_{n-1}$ and $\mathbf{O}_{ob}^{\mathrm{D}} = [\mathbf{O}_{ob};\, \mathbf{E}_{\mathrm{D}}^\top]$, for $T \geq n-1$ we have*

$$\begin{aligned}&\text{rank } \left(\mathbf{O}_{ob}^{\mathrm{D}}\right) = \text{rank } \left(\mathbf{O}_T^{\mathrm{D}}\right)\\ &\text{rank } \left([\mathbf{O}_{ob}^{\mathrm{D}}; \mathbf{e}_i^\top]\right) = \text{rank } \left([\mathbf{O}_T^{\mathrm{D}}; \mathbf{e}_i^\top]\right)\,,\end{aligned}$$

which implies an equivalent and simplified condition of (9) *and (12), respectively by using $\mathbf{O}_{ob}^{\mathrm{D}}$ to replace $\mathbf{O}_T^{\mathrm{D}}$ in* (9) *and (12).*

5 Generic Property of Initial-Value Privacy

In the previous sections, both the differential privacy and unobservability of initial values have been studied from both global and local levels, under a fixed configuration $(\mathbf{A}, \mathbf{C})$ complying with the network structure $(\mathrm{G}, \mathrm{G_S})$. In this section, we aim to explore the effect of the network structure $(\mathrm{G}, \mathrm{G_S})$ on these properties.

In the following, we say a property to be *generically* preserved (or lost) if it is (or is not) fulfilled for *almost all* configurations $(\mathbf{A}, \mathbf{C})$ complying with any non-trivial network structure $(\mathrm{G}, \mathrm{G_S})$, and *fully* preserved (or lost) if such property is (or is not) fulfilled for *all* configurations $(\mathbf{A}, \mathbf{C})$ complying with any non-trivial network structure $(\mathrm{G}, \mathrm{G_S})$. It is clear that these properties are qualitative. Thus, in the following we focus on the qualitative property of the differential initial-value privacy, i.e., with a finite privacy budget $\epsilon \geq 0$ under any fixed $\delta \in (0, 1)$ and $\mu > 0$. Such a qualitative property has been addressed in the previous context to be equivalent to the rank conditions (7) and (10) for the global and local differential initial-value privacy, respectively.

5.1 Generic Global Initial-Value Privacy

In this subsection, we take the system initial values as a whole and study the generic property of differential privacy and unobservability of global initial values $\mathbf{x}_0^{\mathrm{P}}$ for system (1).

Theorem 3 *For system (1), let $\mathrm{P} \subseteq \mathrm{V}$ and Assumption 1 hold.*

(i) The differential privacy of initial values $\mathbf{x}_0^{\mathrm{P}}$ with a finite privacy budget is either preserved generically *or* lost generically*.*

(ii) The unobservability of initial values $\mathbf{x}_0^{\mathrm{P}}$ is exactly either preserved fully *or* lost generically*.*

Theorem 3 demonstrates that the differential privacy and the unobservability of initial values $\mathbf{x}_0^{\mathrm{P}}$ in Definition 1 are both generic *qualitatively*, but subject to some distinctions. By Theorem 3.(ii), given a configuration $(\mathbf{A}, \mathbf{C})$ complying with $(\mathrm{G}, \mathrm{G_S})$ if the unobservability of $\mathbf{x}_0^{\mathrm{P}}$ is lost, then it *must* be lost generically, while if it is preserved then there is no guarantee of preserving such privacy generically. Note that with $\mathrm{P} = \emptyset$, Theorem 3.(ii) is consistent with the classical structural unobservability [19, 20] of system (1), where the unobservability is either *preserved fully* or *lost generically*. This indeed is consistent with Theorem 3.(ii). However, for the differential privacy of $\mathbf{x}_0^{\mathrm{P}}$ with a finite privacy budget, from Theorem 3.(i) if there exists a configuration $(\mathbf{A}, \mathbf{C})$ complying with $(\mathrm{G}, \mathrm{G_S})$ such that it is preserved (or lost), there is no guarantee of preserving (or losing) it generically.

5.2 Generic Local Initial-Value Privacy

In this subsection, we study the generic property of the differential privacy and unobservability of local initial values.

Theorem 4 *Take $i \in \mathrm{P} \subseteq \mathrm{V}$ and let Assumption 1 hold.*

(i) The differential initial-value privacy of node i with a finite privacy budget is either preserved generically *or* lost generically*.*

(ii) The unobservability of node i's initial value is either preserved generically *or* lost generically.

Theorem 4 demonstrates that given any network structure $(\mathrm{G}, \mathrm{G_S})$ and $\mathrm{P} \subset \mathrm{V}$, both the differential initial-value privacy with a finite privacy budget and the unobservability of local node i are either preserved generically or lost generically. Note that the generic property of the local unobservability, in which there is no guarantee of generic preservation (or loss) if there exists a configuration $(\mathbf{A}, \mathbf{C})$ complying with $(\mathrm{G}, \mathrm{G_S})$ such that the local unobservability is preserved (or lost), which is different from the global unobservability addressed in Theorem 3.(ii). To have a better view of this, the following examples are formulated.

Example 2. Consider the unobservability of node 1's initial value with $(\mathbf{A}, \mathbf{C})$ complying with the network structure in Fig. 2. Let the private set $\mathrm{P} = \{1, 2, 3\}$, and the system output trajectory $\mathbf{Y}_T$ with $T = 2$ is given by (2) with

$$\mathbf{O}_T = \begin{bmatrix} c_{11} & 0 & c_{13} \\ 0 & c_{11}a_{12} & 0 \\ c_{11}a_{12}a_{21} & 0 & c_{11}a_{12}a_{23} \end{bmatrix}.$$

It is seen that $\mathbf{O}_T$ is full-rank for almost all configurations $(\mathbf{A}, \mathbf{C})$ complying with Fig. 2. Thus, for any $\mathbf{x}_0, \hat{\mathbf{x}}_0$ with $x_{1,0} \neq \hat{x}_{1,0}$ and $\mathbf{O}_T\mathbf{x}_0 \neq \mathbf{O}_T\hat{\mathbf{x}}_0$ there exists $\mathcal{M} \subseteq \mathrm{range}(\mathscr{M})$ such that $\mathbb{P}(\mathscr{M}(\mathbf{x}_0) \in \mathcal{M}) \neq \mathbb{P}(\mathscr{M}(\hat{\mathbf{x}}_0) \in \mathcal{M})$, for almost all configurations $(\mathbf{A}, \mathbf{C})$ complying with Fig. 2. By Definition 2, this indicates that the initial value of node 1 is observable generically.

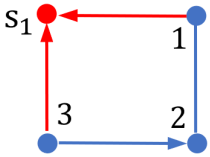

Figure 2. Network topologies $(\mathrm{G}, \mathrm{G_S})$ with 3 network nodes (blue circles) and 1 sensing nodes (red circles). The line without arrow denotes a bidirectional edge.

However, by letting the configuration $(\mathbf{A}, \mathbf{C})$ be such that $c_{11}a_{23} = c_{13}a_{21}$, simple calculations show that $\mathbb{P}(\mathscr{M}(\mathbf{x}_0) \in \mathcal{M}) = \mathbb{P}(\mathscr{M}(\hat{\mathbf{x}}_0) \in \mathcal{M})$ for all $\mathcal{M} \subseteq \mathrm{range}(\mathscr{M})$ and all $\mathbf{x}_0, \hat{\mathbf{x}}_0$ with $x_{1,0} \neq \hat{x}_{1,0}$ and $c_{13}(\hat{x}_{3,0} - x_{3,0}) = c_{11}(x_{1,0} - \hat{x}_{1,0})$. According to Definition 2, this indicates that the initial value of node 1 is unobservable under the configuration $(\mathbf{A}, \mathbf{C})$ satisfying $c_{11}a_{23} = c_{13}a_{21}$.

Thus, even if there exists a configuration such that the initial value of node i is unobservable, it may still be observable generically. This validates the statement (i) of Theorem 4. ■

Example 3. Consider the unobservability of node 4's initial value under the network structure in Fig. 3. Let the private set $\mathrm{P} = \{1, 2, 3, 4\}$, and the output trajectory $\mathbf{Y}_T$ with $T = 3$ is given by (2) with

$$\mathbf{O}_T = \begin{bmatrix} c_{11} & 0 & c_{13} & 0 \\ c_{11}a_{11} & c_{11}a_{12} & 0 & c_{11}a_{14} \\ c_{11}a_{11}^2 & c_{11}a_{12}(a_{11}+a_{22}) & c_{11}a_{12}a_{23} & c_{11}a_{11}a_{14} \\ c_{11}a_{11}^3 & * & ? & c_{11}a_{11}^2a_{14} \end{bmatrix}$$

with $* = c_{11}a_{12}(a_{11}^2 + a_{11}a_{22} + a_{22}^2)$ and $? = c_{11}a_{12}a_{23}(a_{11} + a_{22})$. Simple calculations then can show that $\mathbb{P}(\mathscr{M}(\mathbf{x}_0) \in \mathcal{M}) = \mathbb{P}(\mathscr{M}(\hat{\mathbf{x}}_0) \in \mathcal{M})$ for all $\mathcal{M} \subseteq \mathrm{range}(\mathscr{M})$ and any $\mathbf{x}_0, \hat{\mathbf{x}}_0$ with $x_{4,0} \neq \hat{x}_{4,0}$ and $\hat{x}_{j,0} = x_{j,0} + \eta_j$ for $j = 1, 2, 3$, where η_j's satisfy

$$\begin{aligned} &c_{11}\eta_1 + c_{13}\eta_3 = 0 \\ &a_{11}\eta_1 + a_{12}\eta_2 = a_{14}(x_{4,0} - \hat{x}_{4,0}) \\ &a_{22}\eta_2 + a_{23}\eta_3 = 0\,. \end{aligned} \tag{14}$$

It is clear that the above matrix equations (14) have a solution for almost all configurations $(\mathbf{A}, \mathbf{C})$ complying with Fig. 3, which, by Definition 2, indicates that the initial value of node 4 is unobservable generically.

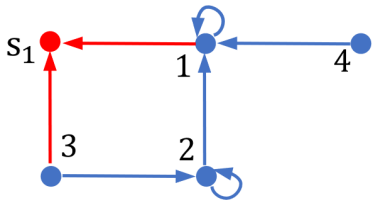

Figure 3. Network topologies $(\mathrm{G}, \mathrm{G_S})$ with 4 network nodes (blue circles) and 1 sensing nodes (red circles).

However, by letting the configuration $(\mathbf{A}, \mathbf{C})$ be such that $c_{13}a_{11}a_{22} + c_{11}a_{12}a_{23} = 0$ and $c_{11}a_{14}a_{22} \neq 0$, it can be seen that there exists no η_j's such that the matrix equations (14) holds for any $x_{4,0} \neq \hat{x}_{4,0}$, and

$$(a_{22}+a_{11})\mathbf{y}_1 - a_{11}a_{22}\mathbf{y}_0 - \mathbf{y}_2 = c_{11}a_{14}a_{22}x_{4,0} + g(\mathbf{W}_T, \mathbf{V}_T)$$

with $g(\mathbf{W}_T, \mathbf{V}_T)$ being some function of noise vectors $\mathbf{W}_T, \mathbf{V}_T$. This immediately yields that for any $\mathbf{x}_0, \hat{\mathbf{x}}_0$ with $x_{4,0} \neq \hat{x}_{4,0}$ there exists $\mathcal{M} \subseteq \mathrm{range}(\mathscr{M})$ such that $\mathbb{P}(\mathscr{M}(\mathbf{x}_0) \in \mathcal{M}) \neq \mathbb{P}(\mathscr{M}(\hat{\mathbf{x}}_0) \in \mathcal{M})$. By Definition 2, this indicates that the unobservability of node 4's initial value is lost under the configuration $(\mathbf{A}, \mathbf{C})$ satisfying $c_{13}a_{11}a_{22} + c_{11}a_{12}a_{23} = 0$ and $c_{11}a_{14}a_{22} \neq 0$.

Thus, even if there exists a configuration such that the unobservability of node i's initial value is lost, such property may still be preserved generically. This is consistent with the statement (ii) of Theorem 4. ■

Remark 9 *It is noted that all previously established results can be extended to linear systems with time-varying state and output matrices* $\mathbf{A}_t, \mathbf{C}_t$ *by replacing the observability matrix* $\mathbf{O}_T$ *by its time-varying variant* $\widehat{\mathbf{O}} := [\mathbf{C}_0; \mathbf{C}_1\mathbf{A}_0; \cdots; \mathbf{C}_T\mathbf{A}_{T-1}\cdots\mathbf{A}_0]$.

6 Applications to Privacy-Preserving Consensus

In this section, we revisit the privacy-preserving consensus algorithm proposed in [15] over an undirected connected communication graph $\mathrm{G}_{\mathrm{com}} = (\mathrm{V}, \mathrm{E}_{\mathrm{com}})$, which can be described by

$$\mathbf{x}_{t+1} = (\mathbf{I} - \mathbf{L})\mathbf{z}_t\,, \quad \mathbf{z}_t = \mathbf{x}_t + \boldsymbol{\gamma}_t \tag{15}$$

where $\mathbf{x}_t$ is the vector of node states, $\mathbf{z}_t$ is the vector of node messages, and $\boldsymbol{\gamma}_t$ is the random noise satisfying

$$\boldsymbol{\gamma}_t = \begin{cases} \mathbf{v}_0\,, & t = 0 \\ \varphi^t\mathbf{v}_t - \varphi^{t-1}\mathbf{v}_{t-1}\,, & t \geq 1 \end{cases}$$

with $\varphi \in (0,1)$ and $\{\mathbf{v}_t\}$ being i.i.d. Gaussian vectors with zero mean and covariance $\mathbf{I}$, and $\mathbf{L}$ is the Laplacian matrix complying with $\mathrm{G}_{\mathrm{com}}$, i.e., $[\mathbf{L}]_{ij} = [\mathbf{L}]_{ji} \geq 0$, $[\mathbf{L}]_{ij} = 0$ if $(j,i) \notin \mathrm{E}_{\mathrm{com}}$, and $\sum_{i=1,i\neq j}^{n}[\mathbf{L}]_{ij} \leq 1$. Let us arrange the eigenvalues of $\mathbf{A} := \mathbf{I} - \mathbf{L}$ in the decreasing order as $\lambda_1 > \lambda_2 \ldots \geq \lambda_n$ with $\lambda_1 = 1$ and $|\lambda_i| < 1$ for $i = 2, \ldots, n$ by [41]. According to [15], there holds

$$\mathbb{E}\|\mathbf{x}_t - \mathbf{1}_n\mathbf{1}_n^\top\mathbf{x}_0/n\|^2 = o(\rho^t), \quad \rho = \max(\varphi^2, \lambda_2^2, \lambda_n^2)\,. \tag{16}$$

In [15], the initial-value privacy of the algorithm (15) is studied against a malicious node under an observability condition, by employing the estimation covariance matrix as the privacy measure. In the following, we consider a different scenario where some transmission messages and initial values are public and the observability condition is removed, and analyze the corresponding differential privacy and unobservability of initial values.

We suppose that the algorithm (15) runs for a finite $T \geq n-1$ iterations and the eavesdroppers have access to the transmission messages of nodes $m_1, \ldots, m_q$. Then we can obtain the system (1) with

$$\mathbf{C} = [\mathbf{e}_{m_1}, \ldots, \mathbf{e}_{m_q}]^\top\,, \quad \boldsymbol{\nu}_t = \mathbf{A}\boldsymbol{\gamma}_t\,, \quad \boldsymbol{\omega}_t = \mathbf{C}\boldsymbol{\gamma}_t\,.$$

With a bit abuse of notations, we let

$$\Omega_T = \begin{bmatrix} \mathbf{C} & 0 & 0 & \cdots & 0 \\ \mathbf{C}(\mathbf{A}-\mathbf{I}) & \varphi\mathbf{C} & 0 & \cdots & 0 \\ \mathbf{C}\mathbf{A}(\mathbf{A}-\mathbf{I}) & \varphi\mathbf{C}(\mathbf{A}-\mathbf{I}) & \varphi^2\mathbf{C} & \cdots & 0 \\ \ddots & \ddots & \ddots & \ddots & \vdots \\ \mathbf{C}\mathbf{A}^T(\mathbf{A}-\mathbf{I}) & \varphi\mathbf{C}\mathbf{A}^{T-1}(\mathbf{A}-\mathbf{I}) & \cdots & \cdots & \varphi^T\mathbf{C} \end{bmatrix}.$$

According to Theorem 1, the following result is formulated to demonstrate the differential initial-value privacy of the algorithm (15).

Proposition 1 *Let* $\mathrm{P} \subseteq \mathrm{V}$ *be any private set. Then for all Laplacian matrix* $\mathbf{L}$ *complying with* $\mathrm{G}_{\mathrm{com}}$*, the algorithm (15) preserves the* (ϵ, δ)*-differential privacy of initial values* $\mathbf{x}_0^{\mathrm{P}}$ *under* μ*-adjacency if and only if*

$$\Delta_{\mathrm{P}} \leq \kappa_\epsilon^{-1}(\delta)/\mu \tag{17}$$

with $\Delta_{\mathrm{P}} = \|\Omega_T^\dagger\mathbf{O}_T\mathbf{E}_{\mathrm{P}}\|$.

With Proposition 1, as T increases, it can be verified that a larger lower bound of ϵ is derived from (17) with fixed μ, δ. This, together with (16), implies a trade-off between the differential privacy and computation accuracy, as in the conventional differential privacy-preserving average consensus algorithms [13,14] by perturbing the initial values with random noises. Note that when T converges to infinity, the resulting ϵ grows to infinity. As for the differential initial-value privacy of local node i, Proposition 1 can still be applied by letting $\mathrm{P} = \{i\}$.

On the other hand, given any P and with $\mathrm{D} = \mathrm{V}\backslash\mathrm{P}$, one can compute the corresponding D-*extended* observability matrix $\mathbf{O}_T^{\mathrm{D}}$ and verify (9) in Theorem 1 (respectively, (12) in Theorem 2) to conclude whether the global (respectively, local) unobservability for the algorithm (15) is preserved. About the generic property, the following result is formulated.

Proposition 2 *The initial values* $\mathbf{x}_0^{\mathrm{P}}$ *of (15) are observable generically, i.e., for almost all Laplacian matrix* $\mathbf{L}$ *complying with the undirected network* $\mathrm{G}_{\mathrm{com}}$.

In summary of the previous analysis, we have established a series of new insights on the differential privacy and unobservability of initial values for the algorithm (15), which together with [15] forms a deep understanding of the initial-value privacy for the algorithm (15).

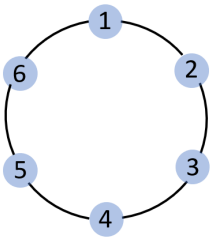

Figure 4. Cycle graph of 6 nodes

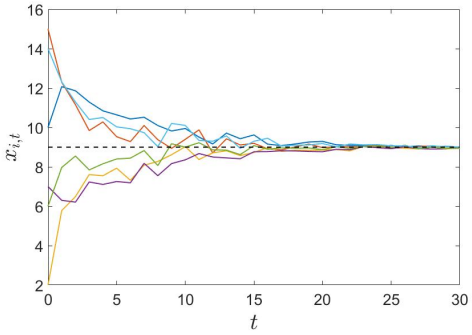

Figure 5. Trajectory of each state $x_{i,t}$. The black dashed line corresponds to the average value.

Example 4. We consider the cycle graph of 6 nodes as in Fig. 4. We assign each edge (i, j) with the same weight $\frac{1}{6}$ and choose $\varphi = 0.9$. Fig. 5 illustrates the trajectory of each node state $x_{i,t}$ with $T = 30$, and $\|\mathbf{x}_T - \mathbf{1}_n\mathbf{1}_n^\top\mathbf{x}_0/n\| = 0.0954$. We assume that the message of node 1 is public, i.e., $\mathbf{C} = \mathbf{e}_1^\top$. Regarding the differential privacy of the algorithm, we let $\mu = 1$ and $\delta = 0.01$, and then can obtain $\epsilon = 797.6$ for $\mathrm{P} = \{1, \ldots, 6\}$, and $\epsilon = 663.1$ for $\mathrm{P} = \{1, 3, \ldots, 6\}$ from (17). As far as the differential privacy of local initial values is concerned, the resulting local ϵ_i with $\mathrm{P} = \{1, 3, \ldots, 6\}$ are given by

$$\epsilon_1 = 195.5,\ \epsilon_3 = 134,\ \epsilon_4 = 127.2,\ \epsilon_5 = 134,\ \epsilon_6 = 155.4.$$

We note that all these privacy levels can be lowered for better privacy guarantees by reducing the running time to $T = 15$, as $\epsilon = 86.0$ for $\mathrm{P} = \{1, \ldots, 6\}$, and for $\mathrm{P} = \{1, 3, \ldots, 6\}$, $\epsilon = 72.1$ and

$$\epsilon_1 = 45.8,\ \epsilon_3 = 10.0,\ \epsilon_4 = 7.3,\ \epsilon_5 = 10.0,\ \epsilon_6 = 20.4,$$

while the computation accuracy becomes larger as $\|\mathbf{x}_T - \mathbf{1}_n\mathbf{1}_n^\top\mathbf{x}_0/n\| = 0.5885$. This thus demonstrates the trade-off between the differential privacy and the accuracy.

Regarding the unobservability, the observability matrix satisfies $\mathrm{rank}\,(\mathbf{O}_T) = 4$. Besides, we have

$$\mathrm{rank}\,\left([\mathbf{O}_T;\, \mathbf{e}_i^\top]\right) = 5\,, \text{for } i = 2, 3, 5, 6,$$

yielding that the unobservability of initial values of all nodes except $1, 4$ is preserved by Theorem 2. We assume that $x_{2,0}$ (or $x_{6,0}$) is public to the eavesdropper, i.e., $\mathrm{D} = \{2\}$ (or $\{6\}$), under which we have $\mathbf{O}_T^{\mathrm{D}} = 5$ and

$$\mathrm{rank}\,\left([\mathbf{O}_T^{\mathrm{D}};\, \mathbf{e}_i^\top]\right) = 6\,, \text{for } i = 3, 5,$$

yielding that the unobservability of initial values of nodes $3, 5$ is preserved and of node 6 (or 2) is lost w.r.t. $\mathrm{D} = \{2\}$ (or $\{6\}$). Thus, the unobservability of initial values of nodes 2 and 6 are closely related, i.e., to protect the unobservability of nodes 2 (or 6), extra measures should be taken to protect $x_{6,0}$ (or $x_{2,0}$) being public. Similarly, it is verified that the unobservability of initial values of nodes $2, 6$ is preserved and of node 5 (or 3) is lost w.r.t. $\mathrm{D} = \{3\}$ (or $\{5\}$). Thus, the unobservability of nodes 3 and 5 are closely related.

7 Conclusions

In this paper, we have studied the differential privacy and unobservability of certain sensitive initial values for linear dynamical systems with random process and measurement noises where the non-sensitive initial values are assumed to be public. We developed necessary and sufficient conditions for both differential initial-value privacy and unobservability, which demonstrates their independent relationship. Particularly, for the differential initial-value privacy both qualitative and quantitative conditions were developed, characterizing the effect of the observability matrix reduced by the set of sensitive initial states on the noise structure and the achievable privacy levels by the noises, respectively. In contrast, it was shown that the unobservability equals to that such a reduced observability matrix is not full-rank. Next, by regarding the considered linear system as a network system, the previously established results have been extended to establish the differential initial-value privacy and unobservability of local nodes. In addition, we showed that all these initial-value properties are generically determined by the network structure from a qualitative perspective. In future works, topological conditions (see e.g. [21, 42]) will be explored for generic global and local unobservability, and the considered privacy metrics will be utilized to develop privacy-preservation approaches for linear dynamical systems.

A Proof of Theorem 1

We notice from the necessary and sufficient conditions (7)-(8) and (9) that the differential privacy of initial values $\mathbf{x}_0^{\mathrm{P}}$ with any privacy levels (ϵ, δ, μ) neither implies nor is implied by the unobservability of $\mathbf{x}_0^{\mathrm{P}}$, demonstrating their independent properties. Thus, we focus on proving the statements (i) and (ii) in the following.

A.1 Proof of statement (i)

The proof is established on the following lemma, adapted from [40, Theorem 8].

Lemma 1 *For any $\epsilon \geq 0, \delta \in (0,1), \mu > 0$, the Gaussian mechanism $M(x) = Fx + Z$ with $Z \sim \mathcal{N}(0, \mathbf{I}_n)$ is (ϵ, δ)-differentially private under μ-adjacency if and only if*

$$\kappa(\epsilon, \mu\|F\|) \leq \delta\,. \tag{A.1}$$

With this lemma in mind, and noting that (A.1) is equivalent to the inequality

$$\|F\| \leq \kappa_\epsilon^{-1}(\delta)/\mu\,,$$

we now proceed to prove the statement (i) of Theorem 1. Let rank $(\Omega_T) = r_{\mathrm{n}}$, and define the orthogonal matrix

$$\mathbf{U} := [\mathbf{U}_1\ \mathbf{U}_2] \in \mathbb{R}^{(m(T+1))\times(m(T+1))}$$

where $\mathbf{U}_1 \in \mathbb{R}^{(m(T+1))\times(m(T+1)-r_{\mathrm{n}})}$ and $\mathbf{U}_2 \in \mathbb{R}^{m(T+1)\times r_{\mathrm{n}}}$ are the matrices, whose columns are eigenvectors corresponding to zero and nonzero eigenvalues of matrix $\Omega_T\Omega_T^\top$, respectively. Thus, we have $\mathbf{U}_1^\top\Omega_T\Omega_T^\top\mathbf{U}_1 = 0$ and $\Lambda_T := \mathbf{U}_2^\top\Omega_T\Omega_T^\top\mathbf{U}_2$ is a nonsingular diagonal matrix. Then we define two mappings

$$\begin{aligned}\mathscr{M}_1(\mathbf{x}_0) &:= \mathbf{U}_1^\top\mathscr{M}(\mathbf{x}_0)\\ \mathscr{M}_2(\mathbf{x}_0) &:= \Lambda_T^{-1/2}\mathbf{U}_2^\top\mathscr{M}(\mathbf{x}_0)\end{aligned}$$

With this in mind, we notice that for any $\mathbf{x}_0, \hat{\mathbf{x}}_0$ satisfying $\mathbf{x}_0^{\mathrm{D}} = \hat{\mathbf{x}}_0^{\mathrm{D}}$ and $\|\mathbf{x}_0^{\mathrm{P}} - \hat{\mathbf{x}}_0^{\mathrm{P}}\| \leq \mu$, (3) is equivalent to saying

$$\begin{aligned}&\mathbb{P}(\mathscr{M}_1(\mathbf{x}_0) \in \mathcal{M}_1)\mathbb{P}(\mathscr{M}_2(\mathbf{x}_0) \in \mathcal{M}_2)\\ &\leq e^\epsilon\mathbb{P}(\mathscr{M}_1(\hat{\mathbf{x}}_0) \in \mathcal{M}_1)\mathbb{P}(\mathscr{M}_2(\hat{\mathbf{x}}_0) \in \mathcal{M}_2) + \delta\,,\\ &\qquad \forall \mathcal{M}_1 \subseteq \mathbb{R}^{m(T+1)-r_n}, \mathcal{M}_2 \subseteq \mathbb{R}^{r_n}\,.\end{aligned} \tag{A.2}$$

In view of the above analysis, the proof reduces to show that (A.2) holds if and only if (7) and (8) are satisfied.

(7)-(8) $\Longrightarrow$ (A.2). With (7), it immediately follows that $\Gamma\mathbf{O}_T\mathbf{E}_{\mathrm{P}} = 0$ for any $\Gamma \in \mathbb{R}^{1\times m(T+1)}$ such that $\Gamma\Omega_T = 0$. As $\mathbf{U}_1^\top\Omega_T\Omega_T^\top\mathbf{U}_1 = 0$, we then can obtain that $\mathscr{M}_1$ is deterministic and $\mathbf{U}_1^\top\mathbf{O}_T\mathbf{E}_{\mathrm{P}} = 0$, implying $\mathbf{U}_1^\top\mathbf{O}_T(\mathbf{x}_0 - \hat{\mathbf{x}}_0) = 0$. This further yields

$$\mathbb{P}(\mathscr{M}_1(\mathbf{x}_0) \in \mathcal{M}_1) = \mathbb{P}(\mathscr{M}_1(\hat{\mathbf{x}}_0) \in \mathcal{M}_1) \in \{0, 1\}\,. \tag{A.3}$$

Moreover, we observe that $\Omega_T^\top\Omega_T = \mathbf{U}_2\Lambda_T\mathbf{U}_2^\top$, which implies $(\Omega_T\Omega_T^\top)^\dagger = \mathbf{U}_2\Lambda_T^{-1}\mathbf{U}_2^\top$ and thus $\sqrt{(\Omega_T\Omega_T^\top)^\dagger} = \Lambda_T^{-1/2}\mathbf{U}_2^\top$. According to Lemma 1, we then can conclude from (8) that the mapping

$$\mathscr{M}_3(\mathbf{x}_0^{\mathrm{P}}) := \Lambda_T^{-1/2}\mathbf{U}_2^\top\mathbf{O}_T\mathbf{E}_{\mathrm{P}}\mathbf{x}_0^{\mathrm{P}} + \boldsymbol{\eta}$$

with $\boldsymbol{\eta} \sim \mathcal{N}(0, \mathbf{I}_{r_n})$, is (ϵ, δ)-differential private under μ-adjacency. Note that $\mathscr{M}_2(\mathbf{x}_0)$ can be rewritten as

$$\mathscr{M}_2(\mathbf{x}_0) = \mathscr{M}_3(\mathbf{x}_0^{\mathrm{P}}) + \Lambda_T^{-1/2}\mathbf{U}_2^\top\mathbf{O}_T\mathbf{E}_{\mathrm{D}}\mathbf{x}_0^{\mathrm{D}}\,.$$

Thus, $\mathscr{M}_2(\mathbf{x}_0)$ is also (ϵ, δ)-differential private under μ-adjacency, i.e.,

$$\begin{aligned}&\mathbb{P}(\mathscr{M}_2(\mathbf{x}_0) \in \mathcal{M}_2) \leq e^\epsilon\mathbb{P}(\mathscr{M}_2(\hat{\mathbf{x}}_0) \in \mathcal{M}_2) + \delta\,,\\ &\qquad \forall \mathcal{M}_2 \subseteq \mathbb{R}^{r_n}\,.\end{aligned} \tag{A.4}$$

Therefore, by combining (A.3) and (A.4), the (A.2) immediately follows.

(A.2) $\Longrightarrow$ (7)-(8). We first prove that (A.2) implies (7) by contradiction. We suppose (7) is not satisfied, i.e.,

$$\text{rank}\,(\Omega_T) \neq \text{rank}\,(\begin{bmatrix}\Omega_T & \mathbf{O}_T\mathbf{E}_{\mathrm{P}}\end{bmatrix})\,. \tag{A.5}$$

It then follows that $\mathbf{U}_1^\top\mathbf{O}_T\mathbf{E}_{\mathrm{P}} \neq 0$, and thus there exist $\mathbf{x}_0, \hat{\mathbf{x}}_0$ satisfying $\mathbf{x}_0^{\mathrm{D}} = \hat{\mathbf{x}}_0^{\mathrm{D}}$ and $\|\mathbf{x}_0^{\mathrm{P}} - \hat{\mathbf{x}}_0^{\mathrm{P}}\| \leq \mu$ such that $\mathbf{U}_1^\top\mathbf{O}_T(\mathbf{x}_0 - \hat{\mathbf{x}}_0) \neq 0$. With such $\mathbf{x}_0, \hat{\mathbf{x}}_0$ being the case, we let $\mathcal{M}_1$ be such that $\mathbf{U}_1^\top\mathbf{O}_T\mathbf{x}_0 \in \mathcal{M}_1$ and $\mathbf{U}_1^\top\mathbf{O}_T\hat{\mathbf{x}}_0 \notin \mathcal{M}_1$, and $\mathcal{M}_2 = \mathbb{R}^{r_n}$. This yields that

$$\begin{aligned}&\mathbb{P}(\mathscr{M}_1(\mathbf{x}_0) \in \mathcal{M}_1)\mathbb{P}(\mathscr{M}_2(\mathbf{x}_0) \in \mathcal{M}_2) = 1\\ &\mathbb{P}(\mathscr{M}_1(\hat{\mathbf{x}}_0) \in \mathcal{M}_1)\mathbb{P}(\mathscr{M}_2(\hat{\mathbf{x}}_0) \in \mathcal{M}_2) = 0\,,\end{aligned}$$

which contradicts with (A.2). Therefore, (7) is satisfied.

With (7), from the previous arguments we can obtain (A.3). This, together with (A.2), then implies that (A.4) must hold, leading to (8) by Lemma 1 and recalling $\sqrt{(\Omega_T\Omega_T^\top)^\dagger} = \Lambda_T^{-1/2}\mathbf{U}_2^\top$.

In summary of the previous proofs, the statement (i) is concluded.

A.2 Proof of statement (ii)

Sufficiency. We suppose (9) holds. Thus, there exists nonzero $\boldsymbol{\eta} \in \ker\left(\mathbf{O}_T^{\mathrm{D}}\right)$ such that $\mathbf{O}_T\mathbf{x}_0 = \mathbf{O}_T(\mathbf{x}_0 + \boldsymbol{\eta})$, which, together with (2), implies

$$\mathbb{P}(\mathscr{M}(\mathbf{x}_0) \in \mathcal{M}) = \mathbb{P}(\mathscr{M}(\mathbf{x}_0 + \boldsymbol{\eta}) \in \mathcal{M}) \tag{A.6}$$

for all $\mathcal{M} \subseteq \text{range}(\mathscr{M})$ and all $\mathbf{x}_0 \in \mathbb{R}^n$. Moreover, given any $\mathbf{x}_0 \in \mathbb{R}^n$, we have $\mathbf{E}_{\mathrm{D}}^\top(\mathbf{x}_0 + \boldsymbol{\eta}) = \mathbf{E}_{\mathrm{D}}^\top \mathbf{x}_0 + \mathbf{E}_{\mathrm{D}}^\top \boldsymbol{\eta} = \mathbf{E}_{\mathrm{D}}^\top \mathbf{x}_0$. This, together with (A.6), completes the proof by Definition 1.(b).

Necessity. To show the necessity part, the contradiction method is used. With the unobservability of $\mathbf{x}_0^{\mathrm{P}}$, we suppose that (9) does not hold, i.e., rank $\left(\mathbf{O}_T^{\mathrm{D}}\right) = n$. Then for all non-identical $\mathbf{x}_0, \hat{\mathbf{x}}_0$ satisfying $\mathbf{x}_0^{\mathrm{D}} = \hat{\mathbf{x}}_0^{\mathrm{D}}$, we have $\mathbf{O}_T^{\mathrm{D}}(\mathbf{x}_0 - \hat{\mathbf{x}}_0) \neq 0$, yielding $\mathbf{O}_T \mathbf{x}_0 \neq \mathbf{O}_T \hat{\mathbf{x}}_0$. Thus, from the definition of $\mathscr{M}$ in (2), it is clear that there exists $\mathcal{M} \subseteq \text{range}(\mathscr{M})$ such that

$$\mathbb{P}(\mathscr{M}(\mathbf{x}_0) \in \mathcal{M}) \neq \mathbb{P}(\mathscr{M}(\hat{\mathbf{x}}_0) \in \mathcal{M}) \,. \tag{A.7}$$

This contradicts with the fact that the $\mathbf{x}_0^{\mathrm{P}}$ of system (1) is unobservable. Therefore, it can be concluded that (9) holds, completing the proof of statement (ii).

B Proof of Theorem 2

We note from Definition 2 that the local differential initial-value privacy of node i is established on the scenario where initial states of all nodes except node i are known by eavesdroppers. Thus, the proof of Theorem 2.(i) can be easily derived by applying Theorem 1.(i) with $\mathrm{P} = \{i\}$. In the following, we focus on the proof of Theorem 2.(ii).

Necessity. We first use the contradiction method to show that if the initial value of node $i \in \mathrm{P}$ is unobservable, then necessarily (12) holds. Following Definition 2.(b), we fix $\mathbf{x}_0, \hat{\mathbf{x}}_0$ as a pair of initial states satisfying $x_{i,0} \neq \hat{x}_{i,0}$, $x_{j,0} = \hat{x}_{j,0}$ for $j \in \mathrm{D}$, such that

$$\mathbb{P}(\mathscr{M}(\mathbf{x}_0) \in \mathcal{M}) = \mathbb{P}(\mathscr{M}(\hat{\mathbf{x}}_0) \in \mathcal{M}) \tag{B.1}$$

for all $\mathcal{M} \subseteq \text{range}(\mathscr{M})$, and suppose that (12) does not hold, i.e.,

$$\text{rank } \left([\mathbf{O}_T^{\mathrm{D}}; \mathbf{e}_i^\top]\right) = \text{rank } \left(\mathbf{O}_T^{\mathrm{D}}\right)$$

which indicates that there exists $\Gamma_1 \in \mathbb{R}^{m(T+1)}$ and $\Gamma_2 \in \mathbb{R}^{|\mathrm{D}|}$ such that

$$\Gamma_1^\top \mathbf{O}_T + \Gamma_2^\top \mathbf{E}_{\mathrm{D}}^\top = \mathbf{e}_i^\top \,.$$

It then follows from (2) that

$$\begin{aligned} \Gamma_1^\top \mathscr{M}(\mathbf{x}_0) &= \Gamma_1^\top \mathbf{O}_T \mathbf{x}_0 + \Gamma_1^\top (\mathbf{H}_T \mathbf{V}_T + \mathbf{W}_T) \\ &= (\mathbf{e}_i^\top - \Gamma_2^\top \mathbf{E}_{\mathrm{D}}^\top)\mathbf{x}_0 + \Gamma_1^\top (\mathbf{H}_T \mathbf{V}_T + \mathbf{W}_T) \\ &= x_{i,0} - \Gamma_2^\top \mathbf{x}_0^{\mathrm{D}} + \Gamma_1^\top (\mathbf{H}_T \mathbf{V}_T + \mathbf{W}_T) \,. \end{aligned}$$

Thus, by $x_{i,0} \neq \hat{x}_{i,0}$ and $x_{j,0} = \hat{x}_{j,0}$ for $j \in \mathrm{D}$, there exists $\bar{\mathcal{M}} \subseteq \text{range}(\Gamma_1^\top \mathscr{M})$ such that

$$\mathbb{P}(\Gamma_1^\top \mathscr{M}(\mathbf{x}_0) \in \bar{\mathcal{M}}) \neq \mathbb{P}(\Gamma_1^\top \mathscr{M}(\hat{\mathbf{x}}_0) \in \bar{\mathcal{M}}) \,.$$

This contradicts with (B.1). Therefore, the identity (12) must hold, completing the necessity proof.

Sufficiency. We approach the sufficiency proof by constructing a $\hat{\mathbf{x}}_0$ with any given $\mathbf{x}_0$ such that $x_{i,0} \neq \hat{x}_{i,0}$, $x_{j,0} = \hat{x}_{j,0}$ for $j \in \mathrm{D}$, and (4) holds.

With (12), we can obtain that $\mathbf{e}_i^\top \notin \text{span}([\mathbf{O}_T; \mathbf{E}_{\mathrm{D}}^\top])$, and there exists $\mathbf{K} \in \ker([\mathbf{O}_T; \mathbf{E}_{\mathrm{D}}^\top])$ such that

$$\mathbf{O}_T \mathbf{K} = 0 \,, \quad \mathbf{E}_{\mathrm{D}}^\top \mathbf{K} = 0 \,, \quad \mathbf{e}_i^\top \mathbf{K} \neq 0.$$

Then given any $\mathbf{x}_0 \in \mathbb{R}^n$, let $\hat{\mathbf{x}}_0 = \mathbf{x}_0 + \mathbf{K}$, yielding

$$\begin{aligned} &\mathbf{x}_0^{\mathrm{D}} - \hat{\mathbf{x}}_0^{\mathrm{D}} = \mathbf{E}_{\mathrm{D}}^\top (\mathbf{x}_0 - \hat{\mathbf{x}}_0) = -\mathbf{E}_{\mathrm{D}}^\top \mathbf{K} = 0 \\ &\hat{x}_{i,0} = \mathbf{e}_i^\top \hat{\mathbf{x}}_0 = \mathbf{e}_i^\top \mathbf{x}_0 + \mathbf{e}_i^\top \mathbf{K} = x_{i,0} \,. \end{aligned}$$

Moreover, we have

$$\begin{aligned} \mathscr{M}(\mathbf{x}_0) &= \mathbf{O}_T \mathbf{x}_0 + \mathbf{H}_T \mathbf{V}_T + \mathbf{W}_T \\ &= \mathbf{O}_T \mathbf{x}_0 + \mathbf{O}_T \mathbf{K} + \mathbf{H}_T \mathbf{V}_T + \mathbf{W}_T \\ &= \mathbf{O}_T \hat{\mathbf{x}}_0 + \mathbf{H}_T \mathbf{V}_T + \mathbf{W}_T \,, \end{aligned}$$

yielding (B.1). By Definition 2, this thus proves that the initial value of node $i \in \mathrm{P}$ is unobservable, completing the proof.

C Proof of Theorem 3

To ease the subsequent analysis, we collect all edge weights a_{ij}, c_{ij} in a configuration vector $\theta \in \mathbb{R}^N$ with N being the total number of edges in $(\mathrm{G}, \mathrm{G_S})$. In this way, all matrices $\mathbf{A}, \mathbf{C}$ are indeed functions of θ, and so are the resulting Ω_T and $\mathbf{O}_T$.

Instrumental to the proof is the following lemma.

Lemma 2 *Let $\Phi(\theta) \in \mathbb{R}^{n \times m}$ with $m \leq n$ be a matrix each entry of which is a polynomial function of θ. Then there exists a $n_{\mathrm{P}}^{ob} \leq m$ such that*

$$\text{rank } (\Phi(\theta)) = r_{\max} \,, \quad \textit{for almost all } \theta \in \mathbb{R}^N \tag{C.1}$$

$$\text{rank } (\Phi(\theta)) \leq r_{\max} \,, \quad \textit{for all } \theta \in \mathbb{R}^N. \tag{C.2}$$

Proof. The proof of this lemma is to find the maximal value of $\text{rank}(\Phi(\theta))$. Let $\bar{\alpha}_j(\theta) : \mathbb{R}^N \to \mathbb{R}$, $j = 1, \ldots, m$ be such that

$$\det \left(s\mathbf{I} - \Phi(\theta)^\top \Phi(\theta)\right) = \sum_{j=1}^{m} \bar{\alpha}_j(\theta) s^{j-1} + s^{n-l} \,.$$

Note that all $\bar{\alpha}_j(\theta)$ are polynomial functions of θ. We run the following recursive algorithm from $k = 1$ until $r_{\max}$ is found.

Step k**:** Check whether there exists $\theta' \in \mathbb{R}^N$ such that $\bar{\alpha}_k(\theta') \neq 0$. If so, using the fact that analytic functions that are not identically zero vanish only on a zero-measure set, we can conclude that $\bar{\alpha}_k(\theta) \neq 0$ holds for almost all $\theta \in \mathbb{R}^N$. This, together with the fact that $\bar{\alpha}_j(\theta) = 0$ for all $j \leq k-1$ and all $\theta \in \mathbb{R}^N$, indicates that (C.1) and (C.2) hold with $r_{\max} = m - k + 1$. Otherwise, if for all $\theta \in \mathbb{R}^N$, $\bar{\alpha}_k(\theta) = 0$, we then proceed to Step $k+1$.

If at the m-th recursion of the above algorithm, we still cannot find a $\theta \in \mathbb{R}^N$ such that $\bar{\alpha}_m(\theta) \neq 0$, we then can conclude that $r_{\max} = 0$. ■

With this lemma in mind, we now proceed to prove the two statements in Theorem 3 respectively.

Proof of (i). According to Theorem 1.(i), the differential privacy of initial values $\mathbf{x}_0^{\mathrm{P}}$ can be preserved with a finite privacy budget if and only if

$$\text{rank } (\Omega_T(\theta)) = \text{ rank } (\begin{bmatrix} \Omega_T(\theta) & \mathbf{O}_T(\theta)\mathbf{E}_{\mathrm{P}} \end{bmatrix}) . \quad \text{(C.3)}$$

Let $\mathbb{S} \subseteq \mathbb{R}^N$ be such that the above equality (C.3) holds for all $\theta \in \mathbb{S}$ and does not hold for all $\theta \in \mathbb{R}^N \backslash \mathbb{S}$. We now show that either such set $\mathbb{S}$ or its complementary set $\mathbb{R}^N \backslash \mathbb{S}$ is zero-measure, which in turn proves the statement (i). In the following, the contradiction method is applied by assuming that both $\mathbb{S}$ and $\mathbb{R}^N \backslash \mathbb{S}$ are nonzero-measure.

Note that each entry of $\Omega_T(\theta)$ and $\mathbf{O}_T(\theta)$ is indeed a polynomial function of θ. By Lemma 2 there exist $\mathbb{S}^{'} \subseteq \mathbb{R}^N$ and $\mathbb{S}^{''} \subseteq \mathbb{R}^N$ such that both $\mathbb{R}^N \backslash \mathbb{S}^{'}$ and $\mathbb{R}^N \backslash \mathbb{S}^{''}$ are zero-measure sets, and

$$\begin{aligned}
&\text{rank } (\Omega_T(\theta)) \leq r_{omega} , && \forall \theta \in \mathbb{R}^N \\
&\text{rank } (\Omega_T(\theta)) = r_{omega} , && \forall \theta \in \mathbb{S}^{'} \\
&\text{rank } (\begin{bmatrix} \Omega_T(\theta) & \mathbf{O}_T(\theta)\mathbf{E}_{\mathrm{P}} \end{bmatrix}) \leq r_{mix} , && \forall \theta \in \mathbb{R}^N \\
&\text{rank } (\begin{bmatrix} \Omega_T(\theta) & \mathbf{O}_T(\theta)\mathbf{E}_{\mathrm{P}} \end{bmatrix}) = r_{mix} , && \forall \theta \in \mathbb{S}^{''}
\end{aligned}$$

for some $r_{omega}, r_{mix} > 0$. As $\mathbb{S}$ is assumed to be nonzero-measure, it then can be seen that $\mathbb{S} \cap \mathbb{S}^{'}$ is nonzero-measure, and thus $\mathbb{S} \cap \mathbb{S}^{'} \cap \mathbb{S}^{''}$ is also nonzero-measure. Note that for all θ in such nonzero-measure set $\mathbb{S} \cap \mathbb{S}^{'} \cap \mathbb{S}^{''}$, there holds the equality (C.3) with rank $(\Omega_T(\theta)) = r_{omega}$ and rank $(\begin{bmatrix} \Omega_T(\theta) & \mathbf{O}_T(\theta)\mathbf{E}_{\mathrm{P}} \end{bmatrix}) = r_{mix}$, which yields that $r_{omega} = r_{mix}$, i.e., (C.3) holds for all $\theta \in \mathbb{S}^{'} \cap \mathbb{S}^{''}$. Hence, it can be concluded that $\mathbb{S}^{'} \cap \mathbb{S}^{''} \subseteq \mathbb{S}$, and thus $\mathbb{R}^N \backslash \mathbb{S} \subseteq \mathbb{R}^N \backslash \mathbb{S}^{'} \cup \mathbb{R}^N \backslash \mathbb{S}^{''}$. Recalling that both $\mathbb{R}^N \backslash \mathbb{S}^{'}$ and $\mathbb{R}^N \backslash \mathbb{S}^{''}$ are zero-measure, we then can obtain that $\mathbb{R}^N \backslash \mathbb{S}$ is also zero-measure, which contradicts with the assumption that both $\mathbb{S}$ and $\mathbb{R}^N \backslash \mathbb{S}$ are nonzero-measure. Therefore, either $\mathbb{S}$ or $\mathbb{R}^N \backslash \mathbb{S}$ is zero-measure, which completes the proof of (i).

Proof of (ii). According to Theorem 1.(ii), the unobservablity of $\mathbf{x}_0^{\mathrm{P}}$ is preserved if and only if

$$\text{rank } \left([\mathbf{O}_T(\theta); \mathbf{E}_{\mathrm{D}}^{\top}] \right) < n . \quad \text{(C.4)}$$

Note that each entry of $\mathbf{O}_T(\theta)$ is a polynomial function of θ. Denote the maximal rank of matrix $[\mathbf{O}_T(\theta); \mathbf{E}_{\mathrm{D}}^{\top}]$ by r_{ob}^{D}. By Lemma 2, it is clear that if there exists one $\theta \in \mathbb{R}^N$ such that $r_{ob}^{\mathrm{D}} = n$, then $r_{ob}^{\mathrm{D}} = n$ for almost all $\theta \in \mathbb{R}^N$, which indicates that the unobservablity of $\mathbf{x}_0^{\mathrm{P}}$ is lost generically. Otherwise, if there does not exist such θ such that $r_{ob}^{\mathrm{D}} = n$, then $r_{ob}^{\mathrm{D}} < n$ for all $\theta \in \mathbb{R}^N$, which indicates that the unobservablity of $\mathbf{x}_0^{\mathrm{P}}$ is preserved fully. This completes the proof.

D Proof of Theorem 4

Proof of (i). The proof of the first statement can be easily done by applying the arguments of the proof for Theorem 3.(i) with $\mathrm{P} = \{i\}$, and is thus omitted for simplicity.

Proof of (ii). Let $\Theta_1 \subseteq \mathbb{R}^N$ be a set of configuration vector θ such that the initial value of node i is unobservable for all $\theta \in \Theta_1$ and observable for all $\theta \in \mathbb{R}^N \backslash \Theta_1$. It is clear that the proof is done if we show that either Θ_1 or $\mathbb{R}^N \backslash \Theta_1$ is zero-measure. To prove it, we use the contradiction method, and assume that there exists a nonzero-measure set $\Theta_1 \in \mathbb{R}^N$ of configuration vector θ such that

- $(P1)$ the set $\mathbb{R}^N \backslash \Theta_1$ is nonzero-measure, and
- $(P2)$ the complete initial-value privacy of node i is preserved only for $\theta \in \Theta_1$ under $(\mathrm{G}, \mathrm{G_S})$, and
- $(P3)$ the complete initial-value privacy of node i is lost for $\theta \in \mathbb{R}^N \backslash \Theta_1$ under $(\mathrm{G}, \mathrm{G_S})$.

Then, according to Theorem 2.(ii) and Remark 7, it can be inferred that

$$(P2) \Longleftrightarrow$$
$$\text{rank } \begin{bmatrix} \mathbf{O}_T(\theta)\mathbf{E}_{\mathrm{P}} \\ \mathbf{e}_i^{\top}\mathbf{E}_{\mathrm{P}} \end{bmatrix} = \text{rank } (\mathbf{O}_T(\theta)\mathbf{E}_{\mathrm{P}}) + 1 , \text{for all } \theta \in \Theta_1 .$$

Let $\alpha_j(\theta):\mathbb{R}^N\to\mathbb{R}$, $j=1,\ldots,n$ be such that

$$\det\left(s\mathbf{I}-\begin{bmatrix}\mathbf{O}_T(\theta)\mathbf{E}_{\rm P}\\ \mathbf{e}_i^\top\mathbf{E}_{\rm P}\end{bmatrix}^\top\begin{bmatrix}\mathbf{O}_T(\theta)\mathbf{E}_{\rm P}\\ \mathbf{e}_i^\top\mathbf{E}_{\rm P}\end{bmatrix}\right)=\sum_{j=1}^{n-l}\alpha_j(\theta)s^{j-1}+s^{n-l}\,.$$

By Lemma 2, there exists a nonzero-measure set $\Theta_{ob}\subseteq\mathbb{R}^N$ such that the set $\mathbb{R}^N\backslash\Theta_{ob}$ is zero-measure, and for all $\theta\in\Theta_{ob}$, rank $(\mathbf{O}_{ob}(\theta)\mathbf{E}_{\rm P})=n_{\rm P}^{ob}$. Besides, it is clear that, for all $\theta\in\mathbb{R}^N$

$$\text{rank}\left(\begin{bmatrix}\mathbf{O}_T(\theta)\mathbf{E}_{\rm P}\\ \mathbf{e}_i^\top\mathbf{E}_{\rm P}\end{bmatrix}\right)\leq\text{rank }(\mathbf{O}_T(\theta)\mathbf{E}_{\rm P})+1\,.\quad\text{(D.1)}$$

Since Θ_1 is nonzero-measure and $\mathbb{R}^N\backslash\Theta_{ob}$ is zero-measure, we have $\Theta_1\cap\Theta_{ob}\neq\emptyset$. Thus letting $\theta^*\in\Theta_1\cap\Theta_{ob}$ yields that rank $(\mathbf{O}_T(\theta^*)\mathbf{E}_{\rm P})=n_{\rm P}^{ob}$ and

$$\begin{aligned}\text{rank}\begin{bmatrix}\mathbf{O}_T(\theta^*)\mathbf{E}_{\rm P}\\ \mathbf{e}_i^\top\mathbf{E}_{\rm P}\end{bmatrix}&=\text{rank }(\mathbf{O}_T(\theta^*)\mathbf{E}_{\rm P})+1\\&=n_{\rm P}^{ob}+1\,.\end{aligned}$$

This then implies $\alpha_{n_{uo}}(\theta^*)\neq 0$ with $n_{uo}=n-l-n_{\rm P}^{ob}$. Note that analytic functions that are not identically zero vanish only on a zero-measure set. This indicates that there is a nonzero-measure set $\Theta_2\subseteq\mathbb{R}^N$ of configuration vector θ such that

($P4$) the set $\mathbb{R}^N\backslash\Theta_2$ is zero-measure, and
($P5$) the inequality $\alpha_{n_{uo}}(\theta)\neq 0$ holds for all $\theta\in\Theta_2$.

Thus, for all $\theta\in\Theta_{ob}\cap\Theta_2$, we have

$$\begin{aligned}\text{rank}\left(\begin{bmatrix}\mathbf{O}_T(\theta)\mathbf{E}_{\rm P}\\ \mathbf{e}_i^\top\mathbf{E}_{\rm P}\end{bmatrix}\right)&\geq n_{\rm P}^{ob}+1\\&=\text{rank }(\mathbf{O}_T(\theta)\mathbf{E}_{\rm P})+1\,,\end{aligned}$$

which, together with (D.1), yields

$$\text{rank}\left(\begin{bmatrix}\mathbf{O}_T(\theta)\mathbf{E}_{\rm P}\\ \mathbf{e}_i^\top\mathbf{E}_{\rm P}\end{bmatrix}\right)=\text{rank }(\mathbf{O}_T(\theta)\mathbf{E}_{\rm P})+1$$

for all $\theta\in\Theta_{ob}\cap\Theta_2$. According to Theorem 2.(ii) and Remark 7, this implies that the initial value of node i is unobservable for all configuration vector $\theta\in\Theta_{ob}\cap\Theta_2$. Then by ($P2$) and ($P3$), it follows that $(\mathbb{R}^N\backslash\Theta_1)\subseteq\mathbb{R}^N\backslash(\Theta_{ob}\cap\Theta_2)$, where the set $\mathbb{R}^N\backslash(\Theta_{ob}\cap\Theta_2)=(\mathbb{R}^N\backslash\Theta_{ob})\cup(\mathbb{R}^N\backslash\Theta_2)$ is zero-measure. This indicates that $\mathbb{R}^N\backslash\Theta_1$ is zero-measure, which contradicts with ($P1$), and thus completes the proof.

E Proof of Proposition 1

Following the terminologies in previous sections, we have

$$\mathbf{Y}_T=\mathbf{O}_T\mathbf{x}_0+\Omega_T\mathbf{v}_{0,\ldots,T}\qquad\text{(E.1)}$$

with $\mathbf{v}_{0,\ldots,T}$ being a vector of i.i.d. noises $\mathbf{v}_t$ over $t\in[0,T]$, satisfying the distribution $\mathcal{N}(0,\mathbf{I})$. Then, it is easily seen that the matrix Ω_T is full-row rank, which indicates that the condition (7) in Theorem 1 is fulfilled for any disclosed set $\mathrm{D}\subset\mathrm{V}$ and all Laplacian matrix $\mathbf{L}$ complying with $\mathrm{G}_{\rm com}$. The proof is thus completed according to Theorem 1.

F Proof of Proposition 2

Following the terminologies in Section 2, we let $(\mathrm{G},\mathrm{G}_{\rm S})$ be the network associated to $(\mathbf{A},\mathbf{C})$ with $\mathbf{A}=\mathbf{I}-\mathbf{L}$. As the communication graph $\mathrm{G}_{\rm com}$ is connected, it is clear that for every node $i\in\mathrm{V}$, there is a directed path from i to a sensor node in $\mathrm{G}_{\rm S}$ in $(\mathrm{G},\mathrm{G}_{\rm S})$. Besides, there exist n disjoint self-cycles (i,i), $i\in\mathrm{V}$ in G as $\mathbf{A}=\mathbf{I}-\mathbf{L}$. Thus, according to Theorem 1 in [20], it is concluded that the pair $(\mathbf{A},\mathbf{C})$ is observable structurally, i.e., for almost all $(\mathbf{A},\mathbf{C})$ complying with $(\mathrm{G},\mathrm{G}_{\rm S})$. Moreover, we collect all edge weights a_{ij} in a configuration vector $\theta\in\mathbb{R}^N$ with N being the total number of edges in G.

With this in mind, we next show that $(\mathbf{I}-\mathbf{L},\mathbf{C})$ is observable for almost all Laplacian matrix $\mathbf{L}$ complying with the communication graph $\mathrm{G}_{\rm com}$, which indeed can be regarded as a generalization of the above analysis on the structural observability of $(\mathbf{A},\mathbf{C})$ by constraining $\theta\in\mathbb{W}:=\{\theta\in\mathbb{R}^N_{\geq 0}:\sum_{j=1}^n a_{ij}(\theta)=1,a_{ij}(\theta)=a_{ji}(\theta),i\in\mathrm{V}\}$, i.e., an algebraic variety of $\mathbb{R}^N$. According to [32, Theorem 3.3 and Remark 1] and the duality between observability and controllability, it follows that $(\mathbf{I}-\mathbf{L},\mathbf{C})$ is observable for almost all Laplacian matrix $\mathbf{L}$ complying with $\mathrm{G}_{\rm com}$. This completes the proof.

References

[1] L. Wang, I. Manchester, J. Trumpf, and G. Shi, "Differential Observability for Initial-Value Privacy of Linear Dynamical Systems," in *Proc. 59th IEEE Conference on Decision and Control (CDC)*, 2020.

[2] J. P. Hespanha, P. Naghshtabrizi, Y. Xu, "A survey of recent results in networked control systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 138-162, 2007.

[3] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787-2805, 2010.

[4] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645-1660, 2013.

[5] M. Kolhe, "Smart grid: Charting a new energy future: Research, development and demonstration," *The Electricity Journal*, vol. 25, pp. 88–93, 2012.

[6] P. Papadimitratos, A. D. La Fortelle, K. Evenssen, R. Brignolo and S. Cosenza, "Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation," *IEEE Communications Magazine*, vol. 47, no. 11, pp. 84-95, 2009.

[7] J. Zhang, F. Wang, K. Wang, W. Lin, X. Xu and C. Chen, "Data-Driven Intelligent Transportation Systems: A Survey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 4, pp. 1624-1639, 2011.

[8] H. Sandberg, G. Dan, and R. Thobaben, "Differentially private state estimation in distribution networks with smart meters," in *Proc. 54th IEEE Conference on Decision and Control*, pp. 4492-4498, 2015.

[9] J. Ma, J. Qin, T. Salsbury, and P. Xu, "Demand reduction in building energy systems based on economic model predictive control," *Chemical Engineering Science*, vol. 67, no.1, pp. 92-100, 2012.

[10] Y. Xu, W. Liu, and J. Gong, "Stable multi-agent-based load shedding algorithm for power systems," *IEEE Transactions on Power Systems*, vol. 26, no. 4, pp. 2006-2014, 2011.

[11] J. Le Ny and G. J. Pappas, "Differentially private filtering," *IEEE Transactions on Automatic Control*, vol. 59, no. 2, pp. 341–354, 2014.

[12] Z. Huang, S. Mitra, and G. Dullerud, "Differentially private iterative synchronous consensus," in *Pro. 2012 ACM Workshop on Privacy in the Electronic Society*, pp. 81–90, ACM, 2012.

[13] E. Nozari, P. Tallapragada and J. Cortes, "Differentially private average consensus: Obstruction, trade-offs, and optimal algorithm design," *Automatica*, vol. 81, pp. 221-231,2017.

[14] J. He, L. Cai, and X. Guan, "Differential private noise adding mechanism and its application on consensus algorithm", *IEEE Transactions on Signal Processing*, vol. 68, pp. 4069-4082, 2020.

[15] Y. Mo and R. M. Murray, "Privacy preserving average consensus," *IEEE Transactions on Automatic Control*, vol. 62, no. 2, pp. 753-765, 2017.

[16] S. Roy, M. Xue and S. K. Das, "Security and discoverability of spread dynamics in cyber-physical networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1694-1707, 2012.

[17] N. E. Manitara and C. N. Hadjicostis, "Privacy-preserving asymptotic average consensus," in *European Control Conference*, pp. 760-765, IEEE, 2013.

[18] C. Altafini. "A system-theoretic framework for privacy preservation in continuous-time multiagent dynamics," *Automatica*, 122: 109253, 2020.

[19] J. L. Willems, "Structural controllability and observability," *Systems & Control Letters*, vol.8, pp.5-12, 1986.

[20] J. M. Dion, C. Commault, F. van der Woude, "Generic properties and control of linear structured systems: a survey," *Automatica*, vol. 39, pp. 1125-1144, 2003.

[21] C. T. Lin, "Structural controllability," *IEEE Transactions on Automatic Control*, vol. 19, no. 3, pp. 201-208, 1974.

[22] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Proc. 3rd Theory of Cryptography Conference*, pp. 265-284, 2006.

[23] C. Dwork, K. Kenthapadi, F. McSherry, I. Mironov, and M. Naor, "Our data, ourselves: Privacy via distributed noise generation," *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 486-503, 2006.

[24] D. Fiore, G. Russo. "Resilient consensus for multi-agent systems subject to differential privacy requirements," *Automatica*, 106: 18-26 , 2019.

[25] X. Liu, J. Zhang, and J. Wang, "Differentially private consensus algorithm for continuous-time heterogeneous multi-agent systems," *Automatica*, 122:109283, 2020.

[26] S. Han, U. Topcu, and G. J. Pappas, "Differentially private distributed constrained optimization," *IEEE Transactions on Automatic Control*, vol. 62, no. 1, pp. 50–64, 2017.

[27] E. Nozari, P. Tallapragada, and J. Cortes, "Differentially private distributed convex optimization via functional perturbation," *IEEE Transactions on Control of Network Systems*, vol. 5, no. 1, pp. 395-408, 2018.

[28] Y. Kawano and M. Cao, "Design of privacy-preserving dynamic controllers," *IEEE Transactions on Automatic Control*, vol. 65, no.9, pp. 3863-3878, 2020.

[29] M. Hale, A. Jones, K.Leahy, "Privacy in feedback: The differentially private LQG," in *Pro. IEEE American Control Conference*, pp. 3386-3391, 2018.

[30] Y. Kawano, K. Kashima, and M. Cao, "Modular control under privacy protection: Fundamental trade-offs," *Automatica*, vol. 127, 109518, 2021.

[31] F. Farokhi, and H. Sandberg, "Ensuring privacy with constrained additive noise by minimizing Fisher information," *Automatica*, vol. 99, pp.275-288, 2019.

[32] T. Menara, D. S. Bassett and F. Pasqualetti, "Structural controllability of symmetric networks", *IEEE Transactions on Automatic Control*, vol. 64, no. 9, pp. 3740-3747, 2019.

[33] T. Boukhobza, F. Hamelin, "Observability analysis for structured bilinear systems: A graph-theoretic approach," *Automatica*, vol. 43, pp. 1968-1974, 2007.

[34] L. Blackhall, and D. Hill, "On the structural controllability of networks of linear systems," in *Proc. 2nd IFAC Workshop on Distributed Estimation and Control in Networked Systems*, pp.245-250, 2010.

[35] S. S. Mousavi, M. Haeri, and M. Mesbahi, "On the structural and strong structural controllability of undirected networks," *IEEE Transactions on Automatic Control*, vol. 63, no. 7, pp. 2234-2241, 2018.

[36] J. Jia, H. J. van Waarde, H. L. Trentelman, and M. K. Camlibel, "A unifying framework for strong structural controllability," *IEEE Transactions on Automatic Control*, vol. 66, no. 1, pp. 391-398, 2021.

[37] F. Pasqualetti, F. Dorfler, and F. Bullo, "Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems" *IEEE Control Systems Magazin*, vol. 35, no. 1, pp. 110-127, 2015

[38] S. Gracy, J. Milošević, and H. Sandberg, "Actuator Security Index for Structured Systems", in Proceedings of *2020 IEEE American Control Conference (ACC)*, pp. 2993–2998, 2020.

[39] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Theoretical Computer Science*, vol. 9, no. 3-4, pp. 211–407, 2013.

[40] B. Balle, Y. Wang, "Improving the Gaussian mechanism for differential privacy: Analytical calibration and optimal denoising," *International Conference on Machine Learning*, pp. 394-403, 2018.

[41] M. Mesbahi, M. Egerstedt. *Graph Theoretic Methods in Multiagent Networks*. Princeton University Press, 2010.

[42] J. M. Hendrickx, M. Gevers, and A. S. Bazanella, "Identifiability of dynamical networks with partial node measurements," *IEEE Transactions on Automatic Control*, vol. 64, no. 6, pp. 2240–2253, 2019.

[43] S. Zhou, J. Lafferty, L. Wasserman. "Compressed and privacy-sensitive sparse regression." *IEEE Transactions on Information Theory*, vol. 55, no. 2, vol. 846-866, 2009.

[44] G. Sugiura, K. Ito, K. Kashima, "Bayesian differential privacy for linear dynamical systems." *IEEE Control Systems Letters*, vol. 6, pp. 896-901, 2022.