Automatica 122 (2020) 109253

Contents lists available at ScienceDirect

Automatica

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

A system-theoretic framework for privacy preservation in continuous-time multiagent dynamics[☆]

Claudio Altafini

Division of Automatic Control, Department of Electrical Engineering, Linköping University, SE-58183, Linköping, Sweden

ARTICLE INFO

Article history:
Received 30 April 2019
Received in revised form 11 June 2020
Accepted 28 July 2020
Available online 24 September 2020

Keywords:
Multiagent dynamics
Privacy preservation
Nonlinear time-varying systems
Lyapunov stability
Average consensus
Synchronization

ABSTRACT

In multiagent dynamical systems, privacy protection corresponds to avoid disclosing the initial states of the agents while accomplishing a distributed task. The system-theoretic framework described in this paper for this scope, denoted dynamical privacy, relies on introducing output maps which act as masks, rendering the internal states of an agent indiscernible by the other agents. Our output masks are local (i.e., decided independently by each agent), time-varying functions asymptotically converging to the true states. The resulting masked system is also time-varying, and has the original unmasked system as its limit system. It is shown that dynamical privacy is not compatible with the existence of equilibria. Nevertheless the masked system retains the same convergence properties of the original system: the equilibria of the original systems become attractors for the masked system but lose the stability property. Application of dynamical privacy to popular examples of multiagent dynamics, such as models of social opinions, average consensus and synchronization, is investigated in detail.

1. Introduction

Most multiagent systems rely intrinsically on collaboration among agents in order to accomplish a joint task. Collaboration however means that exchange of information among the agents cannot be dispensed with. If the information is sensitive, then questions like respecting the privacy of the individual agents naturally rise. Several approaches exist to address this *conundrum* of exchanging information without revealing it. One approach is called differential privacy (Dwork, 2006) and consists, roughly speaking, in corrupting the information being transmitted with a noise from an appropriate distribution so that an observer accessing the transmitted signals can only reconstruct the original data up to a prespecified precision level. Another approach relies on cryptography. Encrypted messages can be exchanged among the agents in various ways, e.g. through trusted third parties (Lazzeretti, Horn, Braca, & Willett, 2014), obfuscation (Ambrosin, Braca, Conti, & Lazzeretti, 2017), or through distributed cryptography schemes (Ruan, Gao, & Wang, 2019). In these approaches the messages from each agent (corrupted with noise or encrypted) are typically exchanged through a communication graph and hence they are available to the other agents of the network. Only the protection mechanism (noise source or cryptographic scheme) is kept private by each agent.

Both approaches have been recently used for multiagent dynamical systems (Cortés et al., 2016; Hale & Egerstedt, 2017; Huang, Mitra, & Dullerud, 2012; Nozari, Tallapragada, & Cortés, 2017; Ny & Pappas, 2014; Ruan et al., 2019). In this case the information to keep private is typically the initial state of the agents. A problem that is often studied in this context is the consensus problem, because it can be used as a basic building block in many distributed algorithms in database computations, sensor fusion, load balancing, clock synchronization, etc. Dynamically, a consensus scheme consists of a stable system in which the final value reached asymptotically is the (weighted) mean of the initial conditions of the agents. A privacy protected consensus should render this value available to all agents while not disclosing the initial conditions themselves to the other agents. For instance, differentially private average consensus schemes are proposed in Gupta, Katz, and Chopra (2017), Huang et al. (2012) and Nozari et al. (2017). Clearly the addition of noise impacts also the performances of the consensus algorithm: convergence to the true value might be missing (Huang et al., 2012) or be guaranteed only in expectation (Nozari et al., 2017). Many other variants are possible: for instance in He, Cai, Cheng, Pan, and Shi (2019), Manitara and Hadjicostis (2013), Mo and Murray (2017) and Rezazadeh and Kia (2018), a non-stochastic perturbation is injected at the nodes, with the constraint that the sum (or integral) over time vanishes. A cryptography-based approach requires instead one or more layers of data encryption technology which must themselves be

☆ Work supported in part by a grant from the Swedish Research Council (Grant No. 2015-04390). The material in this paper was presented at the 58th IEEE Conference on Decision and Control, December 11–13, 2019, Nice, France. This paper was recommended for publication in revised form by Associate Editor Claudio De Persis under the direction of Editor Christos G. Cassandras.

E-mail address: claudio.altafini@liu.se.

https://doi.org/10.1016/j.automatica.2020.109253
0005-1098/

kept secure and protected (Lazzeretti et al., 2014; Ruan et al., 2019). Other system-oriented approaches to privacy protection in distributed computations appear e.g. in Alaeddini, Morgansen, and Mesbahi (2017), Duan, He, Cheng, Mo, and Chen (2015), Liu, Wu, Manchester, and Shi (2019) and Monshizadeh and Tabuada (2019).

The aim of this paper is to propose a conceptually different framework for privacy preservation of the initial states of multiagent dynamics, inspired by system-theoretic considerations. Our framework is exact, and is developed for continuous-time dynamical systems. It relies on what we call *output masks*, i.e., local (in the sense of "agent-local", that is, decided and implemented independently by each agent) time-varying transformations of the states to be transmitted to the neighboring nodes, whose functional form and/or numerical parameters are kept hidden to the other agents. In the privacy literature, the use of masking maps is widespread. For instance, non-invertible maps are used in homomorphic or semi-homomorphic encryption (Farokhi, Shames, & Batterham, 2017; Kogiso & Fujita, 2015; Lazzeretti et al., 2014; Ruan et al., 2019), as well as in secure wiretap channels (Wiese et al., 2016). In the present context, output masks are used to offset the initial condition in a way such that an eavesdropping (curious but not malicious) agent cannot reconstruct it, neither directly nor using a model of the system. In fact, even when an eavesdropper has knowledge of the vector field used by an agent, reconstruction of the initial state of that agent requires to set up a state observer, which in turn requires to identify the functional form and the numerical parameters of the output mask of the agent. In the paper this joint "system identification" and "initial state detection" problem is called *discernibility*, and conditions are given that render the initial state indiscernible.

The approach we follow (offsetting the initial condition) is somewhat related to He et al. (2019), Mo and Murray (2017) and Rezazadeh and Kia (2018). However, our use of output masks enables us to carry out a thorough analysis of the dynamical properties of the masked system, which is novel and insightful of the implications of preserving privacy on the dynamics. When the original unmasked system is globally exponentially stable, or perhaps exponentially stable on "slices" of the state space if there is a continuum of equilibria, as in the consensus problem, we show in the paper that under the assumption that no agent has in-neighborhood that covers that of another agent (Mo & Murray, 2017; Rezazadeh & Kia, 2018), the masked multiagent system globally uniformly converges to the same attractor as the unmasked system while guaranteeing the privacy of the initial conditions at any level of precision.

The price to pay for guaranteeing privacy is that the masked system is time-varying and has no fixed points. However, as long as the output masks are constructed to converge asymptotically to the unmasked state, the masked time-varying system has the original system as its limit system (Artstein, 1976, 1977). When the unmasked system is autonomous, the resulting masked time-varying system is a case of a so-called asymptotically autonomous system (Artstein, 1976; Markus, 1956).

In spite of the indiscernibility of the initial conditions, the asymptotic collapse of the masked dynamics to the original dynamics guarantees that the distributed computation is carried out correctly anyway. Clearly, dealing with a distributed computation representable as a converging dynamical system is a key prerequisite of our method, hence we refer to it as *dynamical privacy*.

The system-theoretical framework for dynamical privacy developed in this paper is for continuous-time multiagent dynamics. Unlike Rezazadeh and Kia (2018), where a similar setting is chosen, we do not require the time integrals of the perturbations to be vanishing asymptotically, which gives us more freedom in the choice of the masks and leads to a framework applicable to a broad range of distributed multiagent scenarios.

In the paper we investigate the effect of output masks on three different case studies: a globally exponentially stable nonlinear system, an average consensus problem, and a system of diffusively coupled higher order ODEs achieving pinning synchronization (Chen, Liu, & Lu, 2007; Yu, Chen, Lü, & Kurths, 2013; Zhou, an Lu, & Lü, 2008). In all three cases a privacy preserving version of the system based on output masks is shown to have the equilibrium point of the unmasked system as unique attractor. However, as the masked system lacks fixed points, it cannot be stable at the attractor. This behavior is designed in purpose. Think for instance at a situation in which the initial conditions are all in a neighborhood of the (say, globally stable) equilibrium point of the unmasked system. If the masked system is stable around that point, its trajectories remain confined in a neighborhood of the equilibrium for all times, leading to an approximate disclosure of the initial states. In order to avoid such situations, a masked system cannot preserve neighborhoods of its attractor, or, in other words, the attractor cannot be also an equilibrium point. To achieve this, our output masks have to be inhomogeneous in the state variables. Such structure is reminiscent of the additive noise used e.g. in differential privacy.

Technically, to show global attractivity in the masked system (in the complement of the agreement subspace for consensus-like problems), we use Lyapunov arguments. The Lyapunov function of the unmasked system is shown to lead to Lyapunov derivatives which are in general sign indefinite, but upper bounded by terms that decay to 0 as $t \to \infty$ (Mu & Cheng, 2005). The reasoning is fundamentally different from those used in stability analysis of time-varying systems (Aeyels & Peuteman, 1998; Lee, Liaw, & Chen, 2001; Loria, Panteley, Popovic, & Teel, 2005), but somehow related to constructions used in input-to-state stability (Sontag & Wang, 1995) and in the stability analysis of nonlinear systems in presence of additive exponentially decaying disturbances (Sussmann & Kokotovic, 1991). In particular, our masked system has a so-called converging-input converging-state property (Sontag, 2003). Boundedness of its trajectories is imposed by choosing Lyapunov functions with globally bounded gradients (Sontag & Krichman, 2003; Teel & Hespanha, 2004). The argument is reminiscent of those used in cascade systems (Chaillet & Angeli, 2008; Panteley & Loria, 1998; Saberi, Kokotovic, & Sussmann, 1990) or in observer-based nonlinear control (Arcak & Kokotovic, 2001).

While the importance of initial conditions is well-known in problems such as average consensus (the final value changes with the initial condition, hence privacy questions are self-evident) in the paper we show that similar privacy issues may arise also in other cases in which the unmasked system is globally exponentially stable. In particular we show that in continuous-time Friedkin–Johnsen models of opinion dynamics (Proskurnikov & Tempo, 2017), the value of the equilibrium point is also a function of the initial conditions, because an inhomogeneous term, depending on the initial conditions, is added to an asymptotically stable linear system. Clearly this is a context in which non-disclosure of the initial states could be of strong relevance.

The case of pinned synchronization is instead an example of an unmasked system which is time-varying (it depends on the pinning exosystem (Yu et al., 2013; Zhou et al., 2008)). Our privacy protection framework applies also to this case, the only difference being that the limit system of the masked system is itself time-varying.

The rest of the paper is organized as follows: a few preliminary results are outlined in Section 2, while the dynamical privacy problem and the properties of the output masks are formulated in Section 3. In Section 4 the case of a globally exponentially stable unmasked system (and the related case of Friedkin–Johnsen opinion dynamics model) is discussed. Sections 5 and 6 deal with privacy preservation respectively for the average consensus problem and for a pinning synchronization problem. The proofs of all results are gather in Appendix.

In the conference version of this paper, Altafini (2019), only the average consensus problem of Section 5 is discussed. The material of Sections 4 and 6 is presented here for the first time.

2. Preliminaries

A continuous function $\alpha : [0, \infty) \to [0, \infty)$ is said to belong to class $\mathcal{K}_\infty$ if it is strictly increasing and $\alpha(0) = 0$. Subclasses of $\mathcal{K}_\infty$ which are homogeneous polynomials of order i will be denoted $\mathcal{K}^i_\infty$: $\alpha(r) = ar^i$ for some constant $a > 0$. A continuous function $\zeta : [0, \infty) \to [0, \infty)$ is said to belong to class $\mathcal{L}$ if it is decreasing and $\lim_{t\to\infty} \zeta(t) = 0$. In particular, we are interested in $\mathcal{L}$ functions that are exponentially decreasing: $\zeta(t) = ae^{-\delta t}$ for some $a > 0$ and $\delta > 0$. We shall denote such subclass $\mathcal{L}^e \subset \mathcal{L}$. A continuous function $\beta : [0, \infty) \times [0, \infty) \to [0, \infty)$ is said to belong to class $\mathcal{KL}^{i,e}_\infty$ if the mapping $\beta(r, t)$ belongs to class $\mathcal{K}^i_\infty$ for each fixed t and to class $\mathcal{L}^e$ for each fixed r, i.e., $\beta(r, t) = ar^i e^{-\delta t}$ for some $a > 0$ and $\delta > 0$.

Consider

$$\dot{x} = g(t, x), \qquad x(t_o) = x_o \tag{1}$$

where $g : \mathbb{R}_+ \times \mathbb{R}^n \to \mathbb{R}^n$ is Lipschitz continuous in x, measurable in t, and such that for each $x_o \in \mathbb{R}^n$ and each $t_o \in \mathbb{R}_+$ the solution of (1), $x(t, x_o)$, exists in $[0, \infty)$. A point $x^* \in \mathbb{R}^n$ is an equilibrium point of (1) if $g(t, x^*) = 0$ for a.e.[1] $t \geq t_o$.

A point $x^* \in \mathbb{R}^n$ is *uniformly globally attractive* for (1) if for each $\nu > 0$ there exists $T = T(\nu) > 0$ such that for each solution $x(t, x_o)$ of (1) it holds that $\|x(t, x_o) - x^*\| < \nu$ for each $t > t_o + T$, each $x_o \in \mathbb{R}^n$ and each $t_o \geq 0$. In particular, if x^* is a uniform global attractor for (1), then as $t \to \infty$ all trajectories $x(t, x_o)$ converge to x^* uniformly in t for all $t_o \geq 0$ and x_o. A point x^* can be attractive for (1) without being an equilibrium of (1) (we will use this fact extensively in the paper).

Given (1), denote $g_s(t, x)$ the translate of $g(t, x)$: $g_s(t, x) = g(t + s, x)$. A (possibly time-dependent) system $\dot{x} = \tilde{g}(t, x)$ is called a *limit system* of (1) if there exists a sequence $\{s_k\}$, $s_k \to \infty$ as $k \to \infty$, such that $g_{s_k}(t, x)$ converges to $\tilde{g}(t, x)$ (Artstein, 1976). An existence condition for a limit system $\tilde{g}(t, x)$ is given in Lemma 1 of Lee et al. (2001): when $g(t, x)$ is a uniformly continuous and bounded function, then there exist increasing and diverging sequences $\{s_k\}$ such that on compact subsets of $\mathbb{R}^n$ $g_{s_k}(t, x)$ converges uniformly to a continuous limit function $\tilde{g}(t, x)$ on every compact of $[0, \infty)$, as $k \to \infty$. In general the limit system may not be unique nor time-invariant. However, when it exists unique, then it must be autonomous (Artstein, 1976; Rouche, Habets, & Laloy, 2012) because all translates $g_{s+s'}(t, x)$ must have themselves a limit system hence the latter cannot depend on time. The time-varying system (1) is called *asymptotically autonomous* in this case.

The ω-limit set of $x(t, x_o)$, denoted Ω_{x_o}, consists of all points x^* such that a sequence $\{t_k\}$, with $t_k \to \infty$ when $k \to \infty$, exists for which $\lim_{k\to\infty} x(t_k, x_o) = x^*$. For time-varying systems, if a solution is bounded then the corresponding Ω_{x_o} is nonempty, compact and approached by $x(t, x_o)$. However, it need not be invariant. Only for limit systems the invariance property may hold, although not necessarily (it may fail even for asymptotically autonomous systems, see Artstein, 1976).

[1] Almost every, i.e., except for at most a set of Lebesgue measure 0.

3. Problem formulation

Consider a distributed dynamical system on a graph with n nodes:

$$\dot{x} = f(x), \qquad x(0) = x_o, \tag{2}$$

where $x = \begin{bmatrix} x_1 & \dots & x_n \end{bmatrix}^T \in \mathbb{R}^n$ is a state vector and $f = [f_1 \dots, f_n]^T : \mathbb{R}^n \to \mathbb{R}^n$ is a Lipschitz continuous vector field. Standing assumptions in this paper are that (2) possesses a unique solution continuable on $[0, \infty)$ for all $x_o \in \mathbb{R}^n$ and that information can be exchanged only between first neighbors on the graph, i.e.,

$$\dot{x}_i = f_i(x_i, x_j, j \in \mathcal{N}_i), \qquad i = 1, \dots, n \tag{3}$$

with $\mathcal{N}_i$ the in-neighborhood of node i. Furthermore, to avoid trivial situations, we impose that $\mathcal{N}_i$ is the "essential neighborhood" of agent i (Mo & Murray, 2017), i.e.,

$$f_i(x_i, x_j, j \in \tilde{\mathcal{N}}_i) \neq f_i(x_i, x_j, j \in \mathcal{N}_i) \quad \forall \tilde{\mathcal{N}}_i \subsetneq \mathcal{N}_i, \qquad \forall i = 1 \dots, n. \tag{4}$$

We are interested in cases in which the system (3) has a globally exponentially stable equilibrium point, i.e., $\lim_{t\to\infty} x(t) = x^*$ for all x_o, but also in cases in which the presence of a conservation law (as in the consensus problem) leads to exponential stability on some submanifold depending on the initial conditions, i.e., $\lim_{t\to\infty} x(t) = x^*(x_o)$.

The *privacy preservation problem* consists in using a system like (2) to perform the computation of x^* in a distributed manner, while avoiding to divulgate the initial condition x_o to the other nodes. Clearly this cannot be achieved directly on the system (2) which is based on exchanging the values x_i between the nodes. It can however be achieved if we insert a mask on the value $x(t)$ which preserves convergence to x^*, at least asymptotically. The masks we propose in this paper have the form of time-varying output maps.

3.1. Output masks

Consider a continuously differentiable time-varying output map

$$h : \mathbb{R}_+ \times \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n \qquad (t, x, \pi) \mapsto y(t) = h(t, x(t), \pi) \tag{5}$$

where $y = \begin{bmatrix} y_1 & \dots & y_n \end{bmatrix}^T \in \mathbb{R}^n$ is an output vector of the same size as x, and $\pi \in \mathbb{R}^m$ is a vector of parameters splittable into n subvectors (not necessarily of the same dimension), one for each node of the network: $\pi = \{\pi_1, \dots, \pi_n\}$.

In the following we refer to $h(t, x(t), \pi)$ as an *output mask* and to y as a *masked output*. The state x of the system is first masked into y and then sent to the first out-neighbors on the graph. The original system (2) can therefore be modified into the following *masked system:*

$$\dot{x} = f(y) \tag{6a}$$

$$y = h(t, x, \pi). \tag{6b}$$

Denote $y(t, x_o)$, of components $y_i(t, x_{o,i})$, $i = 1, \dots, n$, the output trajectory of (6) from the initial state x_o, of components $x_{o,i}$. We assume in what follows that the vector field $f(\cdot)$ is publicly known (i.e., each agent knows the shape of the functions $f_1(\cdot), \dots, f_n(\cdot)$) and that each node knows the output trajectories $y_i(t, x_{o,i})$ of its in-neighbors. The state x and the output mask $h(t, x, \pi)$ (functional form plus values of the parameters π) are instead private to each agent, as explained more in detail next.

Definition 1. A C^1 output map h is said a *local mask* if it has components that are local, i.e., P1: $h_i(t, x, \pi) = h_i(t, x_i, \pi_i) \qquad i = 1, \ldots, n.$

The property of locality guarantees that the output map h_i can be independently decided by node i. Both the functional form chosen for $h_i(\cdot)$ and the numerical value of the parameters π_i can therefore remain hidden to the other agents.

The output mask needs also to avoid mapping neighborhoods of a point x^* of (2) (typically an equilibrium point) into themselves. For that, we introduce the following definition.

Definition 2. A C^1 output map h is said to *preserve neighborhoods* of a point x^* if, for all small $\epsilon > 0$, $\|x_o - x^*\| < \epsilon \implies \|h(0, x_o, \pi) - x^*\| < \epsilon$. It is said *not to preserve neighborhoods* otherwise.

These notions are used in the following definition.

Definition 3. A C^1 output map h is said a *privacy mask* if it is a local mask and in addition

P2: $h_i(0, x_i, \pi_i) \neq x_i \ \forall\, x_i \in \mathbb{R}^n$, $i = 1, \ldots, n$;
P3: $h(t, x, \pi)$ does not preserve neighborhoods of any $x \in \mathbb{R}^n$;
P4: $h_i(t, x_i, \pi_i)$ is strictly increasing in x_i for each fixed t and π_i, $i = 1, \ldots, n$.

Property P2 means that $h_i(\cdot)$ has no fixed points. Property P4 resembles a definition of $\mathcal{K}_\infty$ function, but it is in fact more general: $x = 0$ is not a fixed point of h for any finite t, and h need not be nonnegative in x. Monotonicity of h in x (for each fixed π) follows from Property P4 combined with P1. It implies that h is a bijection in x for each fixed t and π, although one that does not preserve the origin. This is meant to avoid that the output mask introduces undesired behavior in the system, like spurious equilibrium points.

In many cases, it will be necessary to impose that the privacy mask converges asymptotically to the true state, i.e., that the perturbation induced by the mask is vanishing.

Definition 4. The output map h is said a *vanishing privacy mask* if it is a privacy mask and in addition

P5: $|h_i(t, x_i, \pi_i) - x_i|$ is decreasing in t for each fixed x_i and π_i, and $\lim_{t\to\infty} h_i(t, x_i, \pi_i) = x_i$ for each fixed π_i, $i = 1, \ldots, n$.

The difference between the true initial condition $x_{o,i}$ and the masked output $h_i(0, x_{o,i}, \pi_i)$ can be used to quantify the level of privacy for agent i. More formally, if $h_i(\cdot)$ is a privacy mask for agent i, we denote $\rho_i(x_{o,i}) = |h_i(0, x_{o,i}, \pi_i) - x_{o,i}|$ the privacy metric of agent i relative to the initial condition $x_{o,i}$, and $\rho(x_o) = \min_{i=1,\ldots,n} \rho_i(x_{o,i})$ the privacy metric of the system relative to the initial condition x_o.

3.2. Examples of output masks

The following are examples of output masks.

Linear mask

$$h_i(t, x_i, \pi_i) = (1 + \phi_i e^{-\sigma_i t}) x_i, \qquad \phi_i \geq 0, \quad \sigma_i > 0 \tag{7}$$

(i.e., $\pi_i = \{\phi_i, \sigma_i\}$). This local vanishing mask is not a proper privacy mask since $h_i(0, 0, \pi_i) = 0$ i.e. the origin is not masked. Notice that all homogeneous maps have this problem (and they fail to escape neighborhoods of x_i).

Additive mask

$$h_i(t, x_i, \pi_i) = x_i + \gamma_i e^{-\delta_i t}, \qquad \delta_i > 0, \quad \gamma_i \neq 0 \tag{8}$$

(i.e., $\pi_i = \{\delta_i, \gamma_i\}$) is a vanishing privacy mask.

Affine mask

$$h_i(t, x_i, \pi_i) = c_i(x_i + \gamma_i e^{-\delta_i t}), \quad c_i > 1, \quad \delta_i > 0, \quad \gamma_i \neq 0 \tag{9}$$

(i.e., $\pi_i = \{c_i, \delta_i, \gamma_i\}$) is also a privacy mask. Since $\lim_{t\to\infty} h_i(t, x_i, \pi_i) = c_i x_i$, it is however not vanishing.

Vanishing affine mask

$$\begin{aligned} h_i(t, x_i, \pi_i) = &(1 + \phi_i e^{-\sigma_i t})(x_i + \gamma_i e^{-\delta_i t}), \\ &\phi_i > 0, \quad \sigma_i > 0, \quad \delta_i > 0, \quad \gamma_i \neq 0 \end{aligned} \tag{10}$$

(i.e., $\pi_i = \{\phi_i, \sigma_i, \delta_i, \gamma_i\}$). This privacy mask is also vanishing. Notice that in vector form, assuming all nodes adopt it, the vanishing affine mask can be expressed as

$$h(t, x, \pi) = (I + \Phi e^{-\Sigma t})(x + e^{-\Delta t}\gamma) \tag{11}$$

where $\Phi = \mathrm{diag}(\phi_1, \ldots, \phi_n)$, $\Sigma = \mathrm{diag}(\sigma_1, \ldots, \sigma_n)$, $\Delta = \mathrm{diag}(\delta_1, \ldots, \delta_n)$, and $\gamma = \begin{bmatrix} \gamma_1 & \ldots & \gamma_n \end{bmatrix}^T$.

The following proposition shows that for these masks the level of privacy (as defined by the metric ρ), can be made arbitrary if each agent chooses π_i in an appropriate way.

Proposition 1. *Given $\lambda > 0$, for each of the privacy masks (8), (9) and (10) the parameters π_i can be chosen locally by each agent i, $i = 1, \ldots, n$, so that $\rho(x_o) > \lambda$ for any x_o.*

By definition of ρ, the choice of parameters π_i in Proposition 1 is compatible with the privacy of the maps $h_i(\cdot)$ (each agent knows its own $x_{o,i}$, hence can compute $\rho_i(x_{o,i})$ without disclosing $x_{o,i}$).

3.3. Dynamically private systems

Consider the system (6), rewritten here for convenience in components ($i = 1, \ldots, n$):

$$\dot{x}_i = f_i(y_i, y_k, k \in \mathcal{N}_i), \qquad x_i(0) = x_{o,i} \tag{12a}$$

$$y_i = h_i(t, x_i, \pi_i). \tag{12b}$$

We would like to understand when an eavesdropping agent j can violate the privacy of agent i, estimating its initial condition $x_{o,i}$. Recall that we are assuming that the agent j knows:

K1: the form of the vector field $f_i(\cdot)$,
K2: the output trajectories of its incoming neighborhood: $y_k(t, x_{o,k})$, $k \in \{\mathcal{N}_j \cup \{j\}\}$, $t \in [t_o, \infty)$,

while instead the following are unknown for agent j:

U1: the form of the output mask $h_i(\cdot)$ and the numerical values of the parameters π_i,
U2: the output trajectories not in its incoming neighborhood: $y_k(t, x_{o,k})$, $k \notin \{\mathcal{N}_j \cup \{j\}\}$.

Because of item U1 above, the problem of estimating $x_{o,i}$ from the output in (12) cannot be cast as a state observability problem, but rather it has to be treated as a joint system identification + observability problem. To characterize this unusual situation we introduce a new concept, discernibility.

Definition 5. The initial condition of agent i, $x_{o,i}$, is said *discernible for agent j* ($j \neq i$) if agent j can estimate $x_{o,i}$ from the knowledge of K1 and K2. It is said *indiscernible for agent j* otherwise. An initial condition x_o is said *indiscernible* if all of its components $x_{o,i}$ are indiscernible for all agents $j \in \{1, \ldots, n\} \setminus \{i\}$.

Indiscernibility refers to the impossibility to solve the joint identification + observation problem of estimating $x_{o,i}$ in (12). It can be imposed using the properties of a privacy mask together with the following Assumption 1 (see Rezazadeh & Kia, 2018 and Mo & Murray, 2017, Corollary 1).

Assumption 1 (*No Completely Covering Neighborhoods*)**.** The system (6) is such that $\{\mathcal{N}_i \cup \{i\}\} \not\subseteq \{\mathcal{N}_j \cup \{j\}\}$, $\forall\ i, j = 1, \dots, n$, $i \neq j$.

Assumption 1 guarantees that no node has complete information of what is going on at the other nodes. This is a condition on the topology of the graph, and therefore a *system* property, rather than simply a property of well-conceived output maps.

Combining indiscernibility with privacy of the output masks, we can formulate the following definition.

Definition 6. The system (6) is called a *dynamically private* version of (2) if

(1) h is a privacy mask;
(2) the solution of (6) exists unique in $[0, \infty)$ and is bounded $\forall\, x_o \in \mathbb{R}^n$;
(3) $\lim_{t\to\infty} y(t) = \lim_{t\to\infty} x(t)$;
(4) indiscernibility of the initial condition is guaranteed.

The next proposition relates indiscernibility to Assumption 1.

Proposition 2. *If the system (6) satisfies conditions 1–3 of Definition 6 and Assumption 1, then it is a dynamically private version of (2).*

Remark 1. From Proposition 1, when a system is dynamically private with any of (8), (9) and (10) as mask, then privacy can be made to hold at an arbitrary level of precision, i.e., given $\lambda > 0$, $\rho(x_o) > \lambda$ can be guaranteed for any x_o only though local choices of the parameters π_i for each agent.

The privacy property P3 of $h(\cdot)$ suggests that in a dynamically private system we cannot have equilibrium points and therefore we cannot talk about stability (of equilibria), while convergence of $y(t)$ to $x(t)$ suggests that as long as $f(\cdot)$ is autonomous, a dynamically private system is asymptotically autonomous with the unmasked system as limit system. This can be shown to be always true if the output mask is vanishing.

Proposition 3. *If (6) is a dynamically private version of (2), then it cannot have equilibrium points. Furthermore, if $h(\cdot)$ is a vanishing privacy mask, then the system (6) is asymptotically autonomous with limit system (2).*

The "vanishing" attribute of the second part of Proposition 3 is sufficient but not necessary. As we will see below, when (2) is globally exponentially stable, the condition that the output mask must be vanishing can be dispensed with.

4. Dynamical privacy in globally exponentially stable systems

In this section we restrict ourselves to unmasked systems (2) having a globally exponentially stable equilibrium point. Under Assumption 1, any privacy mask (not necessarily vanishing) can guarantee privacy of the initial conditions. We will only show the simplest case of affine mask. Since we rely on standard converse Lyapunov theorems, we also request (2) to be globally Lipschitz.

Theorem 1. *Consider the system (2) with $f : \mathbb{R}^n \to \mathbb{R}^n$ globally Lipschitz continuous, $f(0) = 0$, and the masked system (6) with the affine mask*

$$h(t, x, p) = C(x + e^{-\Delta t}\gamma), \tag{13}$$

$C = \mathrm{diag}(c_1, \dots, c_n)$, $c_i > 1$, $\Delta = \mathrm{diag}(\delta_1, \dots, \delta_n)$, $\delta_i > 0$, and $\gamma = \begin{bmatrix}\gamma_1 & \dots & \gamma_n\end{bmatrix}^T$, $\gamma_i \neq 0$. If Assumption 1 holds and the equilibrium $x^* = 0$ is globally exponentially stable for (2), then $x^* = 0$ is uniformly globally attractive for the masked system (6). Furthermore, (6) is a dynamically private version of (2).

Remark 2. Even if (2) has $x^* = 0$ as equilibrium point, the masked system (6) does not, as can be seen from the expression (A.11) in the proof of Theorem 1. This follows from the inhomogeneity of the output mask. Since $x^* = 0$ is not stationary, we cannot talk about stability of its neighborhoods. Nevertheless, x^* remains an attractor for all trajectories of the system.

The following corollary states that the dynamically private system is asymptotically autonomous with ω-limit set identical to that of the corresponding unmasked system.

Corollary 1. *Under the assumptions of Theorem 1, the system (6) with the output mask (13) is asymptotically autonomous with limit system*

$$\dot{x} = f(C^{-1}x). \tag{14}$$

The ω-limit set of each trajectory of (6) is given by $\{0\}$ for each $x_o \in \mathbb{R}^n$.

Notice that since the affine mask (13) is not vanishing, (14) differs from (2) (yet x^* is the same).

Remark 3. The result of Theorem 1 can be rephrased as a converging-input converging-state property (Sontag, 2003): under the assumption of f (locally) Lipschitz continuous and x^* globally asymptotically stable, boundedness of the trajectories is enough to guarantee that $x(t) \to 0$ as $t \to \infty$. However, guaranteeing boundedness is a nontrivial task: a globally asymptotically stable system can be destabilized by an additive perturbation which is arbitrarily small in $\mathcal{L}_1$ norm (Sontag & Krichman, 2003). Similarly, a globally exponentially stable system with linear sector growth (as opposed to global Lipschitzianity) can be destabilized by arbitrarily small additive exponentially decaying disturbances (Astolfi, 2007; Teel & Hespanha, 2004). The assumptions made in Theorem 1 imply the boundedness of the gradient of the Lyapunov function, which in turn guarantees boundedness of the solutions.

Example 1. Consider the following interconnected system with saturated nonlinearities

$$\dot{x} = -x + \kappa A \psi(x) \tag{15}$$

where the off-diagonal matrix $A \geq 0$ is a weighted adjacency matrix of spectral radius $\rho(A) > 0$ describing the interactions among the agents and satisfying Assumption 1, $\kappa > 0$ is a scalar coefficient, and $\psi(x) = \begin{bmatrix}\psi_1(x_1) & \dots & \psi_n(x_n)\end{bmatrix}^T$, $\psi_i(x_i) = \tanh(x_i)$, is a vector of saturated sigmoidal functions depending only on the state of the sending node x_i. The system (15) is used e.g. in Fontan and Altafini (2018) to describe collective distributed decision-making systems. If we impose the condition $\kappa < \frac{1}{\rho(A)}$, then $x^* = 0$ is a globally exponentially stable equilibrium point for (15). In fact, in this case a simple quadratic Lyapunov function $V = \frac{1}{2}\|x\|^2$ leads to

$$\dot{V} = -x^T x + \kappa x^T A \psi(x) \leq x^T(-I + \kappa A)x < 0$$

because $\psi_i(x_i)$ obeys to the sector inequality $0 \leq \psi_i(x_i)x_i \leq 1$. Since the system is globally Lipschitz, Theorem 1 is applicable to it if we choose an output mask like (13). Simulations for $n = 100$ are shown in Fig. 1 for a privacy measure of $\lambda = 1$. Notice in panel (c) how the gap between $x_{o,i}$ and $y_{o,i}$ induced by this privacy level is clearly visible. The initial conditions obey to $\rho_i(x_{o,i}) = |y_i(0) - x_i(0)| \geq 1$, but $|y_i(t) - x_i(t)|$ necessarily decreases as t grows, and converges to 0 as t diverges, see panel (d).

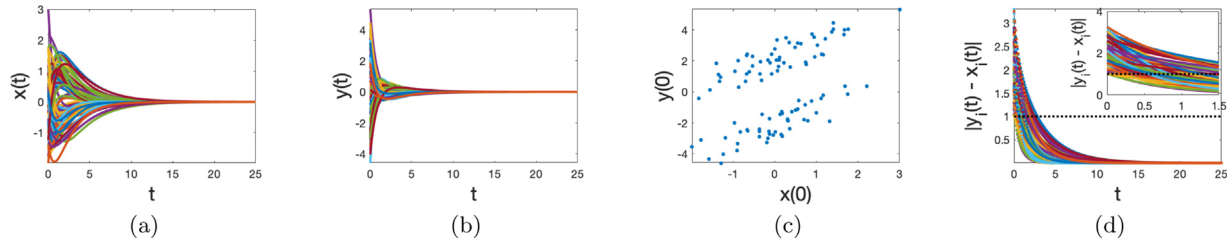

Fig. 1. Privacy-preserving globally exponentially stable system of Example 1. (a): private state $x(t)$; (b): masked output $y(t)$; (c): initial conditions $x(0)$ vs. $y(0)$; (d): $|y_i(t) - x_i(t)|$. The black dotted line in (d) represents λ. The inset of panel (d) is a zoom in of the initial part.

In Example 1 global exponential stability implies that the initial conditions are forgotten asymptotically. In these cases privacy protection might be considered less critical than when the equilibrium point is itself a function of the initial state, as it happens in the next sections.

4.1. Application to continuous-time Friedkin–Johnsen model

Let us consider a continuous-time Friedkin–Johnsen model (also known as Taylor model, see Proskurnikov & Tempo, 2017)

$$\dot{x} = -(L + \Theta)x + \Theta x_o, \qquad x(0) = x_o, \tag{16}$$

where L is an irreducible Laplacian matrix, and $\Theta = \mathrm{diag}(\theta_1, \ldots, \theta_n)$, $\theta_i \in [0,\ 1]$, is a diagonal matrix of so-called susceptibilities, i.e., tendencies of the i-th agent to remain attached to its own initial opinion x_{o_i}. The behavior of the system (16) is analyzed in Proskurnikov and Tempo (2017): when L is irreducible and some $\theta_i \neq 0$, it has a single equilibrium point $x^* = (L+\Theta)^{-1}\Theta x_o$ which is asymptotically stable for a solution starting in x_o. The system reduces to the usual consensus problem when $\theta_i = 0\ \forall\, i$ (see Section 5). Notice how in the affine model (16), the initial opinions (initial condition of the system) enter also in the vector field at time t. Hence protecting the privacy of the agents in (16) requires a 'double mask', i.e., one needs to replace both $x(t)$ and x_o with suitably masked versions $y(t)$ and $y_o = y(0)$ (since y_o is transmitted to the neighboring agents, it can be memorized and used whenever needed).

Denoting $z = x - x^* = x - (L+\Theta)^{-1}\Theta x_o$, then (16) is expressed in z as the linear system

$$\dot{z} = -(L + \Theta)z, \tag{17}$$

which has $z^* = 0$ as globally asymptotically (and hence exponentially) stable equilibrium point, meaning that Theorem 1 is applicable. In the original x basis, a consequence of inhomogeneity of (16) is that the attractor x^* is a function of the initial condition x_o, and it moves with it: $x^* = x^*(x_o)$. To talk rigorously about global asymptotic stability, we should use (17) in z-coordinates. However, for homogeneity of presentation, the next theorem is still formulated in terms of x and y variables, and global asymptotic stability/attractivity is referred to the "moving" point[2] $x^*(x_o)$. Another consequence of the inhomogeneous structure of (16) is that nonvanishing affine privacy masks like the one used in Theorem 1 cannot be used. To obtain convergence to the correct $x^*(x_o)$ we need to use a vanishing privacy mask.

Theorem 2. *If Assumption 1 holds, the masked system*

$$\begin{aligned} \dot{x} &= (-L - \Theta)y + \Theta y_o \\ y &= h(t,\ x,\ \pi) = \left(I + \Phi e^{-\Sigma t}\right)\left(x + e^{-\Delta t}\gamma\right) \end{aligned} \tag{18}$$

where $y_o = h(t,\ x_o,\ \pi)$ and $\Theta \neq 0$, is a dynamically private version of (16). If $x^*(x_o) = (L+\Theta)^{-1}\Theta x_o$ is the globally asymptotically stable equilibrium point of (16), then $x^*(x_o)$ is a globally uniform attractor of (18).

Corollary 2. *The masked system (18) is asymptotically autonomous with (16) as limit system. The ω-limit set of (18) is given by $\{x^*(x_o)\} = \{(L+\Theta)^{-1}\Theta x_o\}$ for each x_o.*

Example 2. An example of $n = 100$ agents is shown in Fig. 2. The introduction of $h(\cdot)$ scrambles the initial conditions, as expected, see panel (c) of Fig. 2. A level of privacy $\lambda = 1$ is requested. Both $x(t)$ and $y(t)$ converge to the same $x^* = (L+\Theta)^{-1}\Theta x_o$, see panel (d) of Fig. 2, although neither now respects the rankings during the transient (i.e., unlike for (16), for (18) it is no longer true that $x_i(t_1) < x_j(t_1) \Longrightarrow x_i(t_2) < x_j(t_2)$ for all $t_2 > t_1$).

5. Dynamically private average consensus

In the average consensus problem, $f(x) = -Lx$, with L a weight-balanced Laplacian matrix: $L\mathbf{1} = L^T\mathbf{1} = 0$, with $\mathbf{1} = \begin{bmatrix}1 & \ldots & 1\end{bmatrix}^T \in \mathbb{R}^n$. When L is irreducible, the equilibrium point is $x^*(x_o) = (\mathbf{1}^T x_o/n)\mathbf{1}$. The system has a continuum of equilibria, described by $\mathrm{span}(\mathbf{1})$, and each $x^*(x_o)$ is globally asymptotically stable in $\mathrm{span}(\mathbf{1})^\perp$, see Olfati-Saber and Murray (2004).

Theorem 3. *Consider the system*

$$\dot{x} = -Lx, \qquad x(0) = x_o \tag{19}$$

where L is an irreducible, weight-balanced Laplacian matrix, and denote $\eta = \mathbf{1}^T x_o/n$ its average consensus value. Then $x^* = \eta\mathbf{1}$ is a global uniform attractor on $\mathrm{span}(\mathbf{1})^\perp$ for the masked system

$$\begin{aligned} \dot{x} &= -Ly \\ y &= h(t,\ x,\ \pi) = \left(I + \Phi e^{-\Sigma t}\right)\left(x + e^{-\Delta t}\gamma\right). \end{aligned} \tag{20}$$

Furthermore, if Assumption 1 holds, then (20) is a dynamically private version of (19).

The proof of this Theorem can be found in Altafini (2019) and is therefore omitted.

Also in this case our masked system is an asymptotically autonomous time-varying system.

Corollary 3. *The masked system (20) is asymptotically autonomous with (19) as limit system. The ω-limit set of (20) is given by $\{\eta\mathbf{1}\}$ for each x_o.*

Remark 4. Even if (19) has $x^* = \eta\mathbf{1}$ as a globally asymptotically stable equilibrium point in $\mathrm{span}(\mathbf{1})^\perp$, the masked system (6) does not have equilibria because of the extra inhomogeneous term on the right hand side , hence we cannot talk about stability of $\eta\mathbf{1}$. Nevertheless, $x^* = \eta\mathbf{1}$ remains a global attractor for all trajectories of the system in $\mathrm{span}(\mathbf{1})^\perp$.

[2] Unlike for the consensus problem which we will study in Section 5, in this case there is no easy way to describe the orthogonal complement of the space in which $x^*(x_o)$ moves.

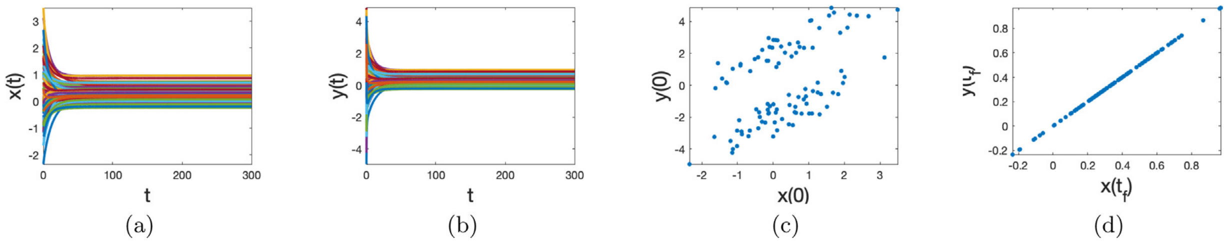

Fig. 2. Privacy-preserving continuous-time Friedkin–Johnsen model of Example 2. (a): private state $x(t)$; (b): masked output $y(t)$; (c): initial condition $x(0)$ vs. $y(0)$; (d): final condition $x(t_f)$ vs. $y(t_f)$, where t_f = final time of the simulation.

Remark 5. Since the evolution of the masked system (19) is restricted to the $n-1$ dimensional subspace $\mathrm{span}(\mathbf{1})^\perp$, our masked consensus problem (as any exact privacy preserving consensus scheme) makes sense only when $n > 2$. The case $n = 2$ never satisfies Assumption 1 when L is irreducible.

Example 3. In Fig. 3 a private consensus problem is run among $n = 100$ agents. Both $x(t)$ and $y(t)$ converge to the same consensus value $\eta = \mathbf{1}^T x(0)/n$, but the initial condition $y(0)$ does not reflect $x(0)$, not even when $x_i(0)$ is already near η ($h(\cdot)$ does not preserve neighborhoods, see panel (c) of Fig. 3). The level of privacy measure imposed in this simulation is $\lambda = 1$. Notice that $\mathbf{1}^T x(t)/n$ is constant over t, while $\mathbf{1}^T y(t)/n$ is not, i.e., the output mask hides also the conservation law. Notice further that a standard Lyapunov function used for consensus, like $V_{mm}(t) = \max_i(x_i(t)) - \min_i(x_i(t))$, does not work in our privacy-preserving scheme (see panel (d) of Fig. 3), which reflects the fact that the system (20) is not asymptotically stable in $\mathrm{span}(\mathbf{1})^\perp$. The convergence speed of the time-dependent part can be manipulated by selecting the factors σ_i and δ_i appropriately.

6. Privacy for higher order systems: the case of pinned synchronization

When instead of a scalar variable, at each node we have a vector of variables $x_i \in \mathbb{R}^\nu$, $\nu > 1$, then the definition of output mask can be straightforwardly extended by defining $h_i(t, x_i, \pi_i)$ as a ν-dimensional diagonal map. For instance for the vanishing affine output mask, in place of (10) at each node we can use

$$h_i(t, x_i, \pi_i) = (I + \Phi_i e^{-\Sigma_i t})(x_i + e^{-\Delta_i t}\gamma_i)$$

where $\Phi_i = \mathrm{diag}(\phi_{i,1}, \ldots, \phi_{i,\nu})$, $\Sigma_i = \mathrm{diag}(\sigma_{i,1}, \ldots, \sigma_{i,\nu})$, $\Delta_i = \mathrm{diag}(\delta_{i,1}, \ldots, \delta_{i,\nu})$, and $\gamma_i = \begin{bmatrix} \gamma_{i,1} & \ldots & \gamma_{i,\nu} \end{bmatrix}^T$. The formalism introduced in the paper extends unaltered.

We will now investigate privacy protection in a standard example of coordination of multivariable multiagent systems: synchronization via pinning control of identical nonlinear systems with diffusive couplings (Chen et al., 2007; Yu et al., 2013; Zhou et al., 2008). Other settings of multiagent coordination can be treated in an analogous way.

Consider a network of n agents obeying the following set of coupled differential equations

$$\dot{x}_i = f(x_i) - \sum_{j=1}^{n} \ell_{ij} R x_j - p_i R(x_i - s), \qquad i = 1, \ldots, k \tag{21}$$

$$\dot{x}_i = f(x_i) - \sum_{j=1}^{n} \ell_{ij} R x_j, \qquad i = k+1, \ldots, n \tag{22}$$

where $x_i \in \mathbb{R}^\nu$, $L = (\ell_{ij})$ is an irreducible Laplacian matrix, and R is a symmetric positive definite matrix of inner couplings. The extra term in the first k equations expresses the coupling with a pinned node (p_i = pinning gain), acting as an exosystem for (21)–(22) and obeying to the law

$$\dot{s} = f(s). \tag{23}$$

The system (23) can represent an equilibrium point, a periodic or a chaotic system (Yu et al., 2013). Synchronization of (21)–(22) to the exosystem (23) corresponds to

$$\lim_{t\to\infty} \|x_i(t) - s(t)\| = 0 \quad \forall\, x_i(0) \in \mathbb{R}^\nu, \quad \forall\, i = 1, \ldots, n.$$

We need the following (standard) assumption:

Assumption 2 (*Global Lipschitzianity of the Drift*)**.** $f : \mathbb{R} \to \mathbb{R}$ is such that

$$\|f(x) - f(z)\| \leq q\big((x-z)^T R (x-z)\big)^{\frac{1}{2}} \qquad \forall\, x, z \in \mathbb{R}^\nu \tag{24}$$

for some positive constant q.

Under Assumption 2, then a sufficient condition for global synchronization of (21)–(22) to (23) is given by the following matrix inequality

$$q\Xi \otimes R - \left(\frac{1}{2}(\Xi L + L^T \Xi) + \Xi P\right) \otimes R < 0 \tag{25}$$

where $\Xi = \mathrm{diag}(\xi)$, with $\xi = (\xi_1, \ldots, \xi_n)$ the left eigenvector of L relative to 0, and $P = \mathrm{diag}(p_1, \ldots, p_k, 0, \ldots, 0)$, see Yu et al. (2013) for more details.

Theorem 4. *Under Assumptions 1 and 2, if the solution $s(t)$ of (23) is bounded $\forall\, t \in [0, \infty)$, L is irreducible, and P is such that (25) holds, then the exosystem (23) is a global attractor for the trajectories of the dynamically private system:*

$$\dot{x}_i = f(y_i) - \sum_{j=1}^{n} \ell_{ij} R y_j - p_i R(y_i - s), \quad i = 1, \ldots, k \tag{26}$$

$$\dot{x}_i = f(y_i) - \sum_{j=1}^{n} \ell_{ij} R y_j, \quad i = k+1, \ldots, n \tag{27}$$

$$y_i = \left(I + \Phi_i e^{-\Sigma_i t}\right)\left(x_i + e^{-\Delta_i t}\gamma_i\right), \quad i = 1, \ldots, n. \tag{28}$$

Remark 6. Notice that the masked system (26)–(28) is not asymptotically autonomous, as its limit system (21)–(22) is a function of the exosystem $s(t)$ which also constitutes the ω-limit set of the system.

Example 4. Consider the case of an $f(\cdot)$ representing a three dimensional chaotic attractor (here the model presented in Zhou et al. (2008) is used). In Fig. 4 a system of $n = 50$ coupled agents synchronize to an exosystem $s(t)$ obeying the same law. The privacy measure in this example is set to $\lambda = 10$. The convergence speed can be tuned by changing the Σ_i and Δ_i parameters of the masks.

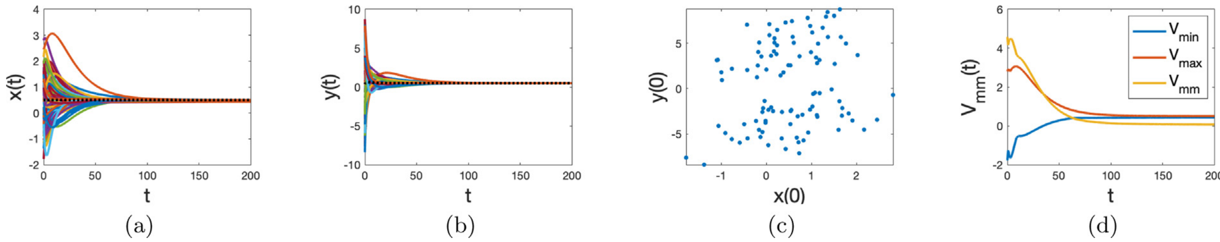

Fig. 3. Privacy-preserving consensus of Example 3. (a): private state $x(t)$; (b): masked output $y(t)$; (c): initial conditions $x(0)$ vs. $y(0)$; (d): $V_{mm}(t) = \max_i(x_i(t)) - \min_i(x_i(t))$. The black dotted line in (a) resp. (b) represents $\mathbf{1}^T x(t)/n$, resp. $\mathbf{1}^T y(t)/n$.

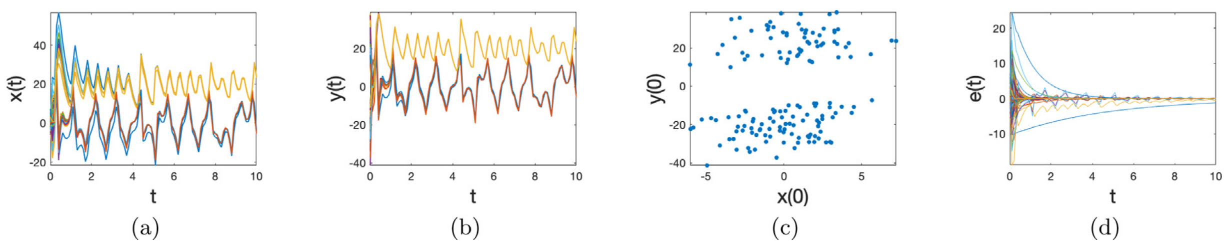

Fig. 4. Privacy-preserving pinned synchronization of Example 4. (a): private state $x(t)$; (b): masked output $y(t)$; (c): initial condition $x(0)$ vs. $y(0)$; (d): error $e(t)$.

7. Conclusions

The approach to privacy protection we have taken in this paper is exact and inspired by classical nonlinear systems techniques. While most of the assumptions under which it holds are fairly simple and reasonable (only the internal state of an agent and the parameters of its output mask must be kept private), the need to have non completely covering neighborhoods (Assumption 1) is instead restrictive, but difficult to dispense with without requiring some other form of restriction (for instance privacy of the vector fields themselves). Assumption 1 is key to guarantee the impossibility for an eavesdropper to identify a model of the system, and hence to set up an observer for x_o. Notice that a breaching of the privacy at one node does not compromise the other nodes.

From a system-theoretical perspective, the most interesting fact described in the paper is that privacy seems incompatible with a point being a fixed point of a dynamical system, as in that case if all agents happen to have initial conditions already on the fixed point, privacy is compromised (an agent will see the same stationary messages being exchanged among its neighboring nodes for all t). By extension of the same argument, approximate privacy (at any level of accuracy) does not seem to be compatible with stability. It is intriguing to investigate if concepts like ϵ-differential privacy (Cortés et al., 2016) can be rephrased in these more dynamical terms.

Several generalizations of our approach are possible. First of all an equivalent framework for discrete-time systems should be developed. Then it is easy to think of output masks that vanish in finite time rather than asymptotically. More complicated seems to be integrating the time dependence introduced by an output mask with a time-varying communication graph. Even more challenging is the case in which, instead of global exponential stability (perhaps on "slices" of the state space if there is a continuum of equilibria) of the unmasked system, this last has multiple isolated locally exponentially stable equilibria. In this case even a transient output mask may lead to tipping over from one basin of attraction to another, hence it should be used with care.

Acknowledgments

The author would like to thank Claudio De Persis for useful discussions on the topic of the paper and the anonymous reviewers for constructive criticisms. This paper is dedicated to the memory of the author's father.

Appendix

A.1. Auxiliary lemmas

The following lemma is inspired by Mu and Cheng (2005), Thm 2.1 and Saberi et al. (1990), Prop. 5, and provides us with a suitable comparison function to be used later in the paper.

Lemma 1. *Consider the scalar system*

$$\dot{v} = -\alpha(v) + \beta(v,t) + \zeta(t), \qquad v(t_o) = v_o \geq 0. \tag{A.1}$$

If $\alpha(v) \in \mathcal{K}^2_\infty$, $\beta \in \mathcal{KL}^{1,e}_\infty$ and $\zeta \in \mathcal{L}^e$, then the solutions of (A.1) are all prolongable to ∞ and bounded $\forall\ v_o \geq 0$ and $\forall t_o \geq 0$. Furthermore,

$$\lim_{t\to\infty} v(t) = 0 \qquad \forall\ v_o \geq 0, \quad \forall\ t_o \geq 0.$$

Proof. It follows from $\alpha(t) \geq 0$, $\beta(v,t) \geq 0$, $\zeta(t) \geq 0$ for all $v > 0$ and $\alpha(0) = 0$ that $\mathbb{R}_+$ is invariant for the system (A.1). If we can show that (A.1) remains bounded for all times, then (A.1) is also forward complete for all $v_o \geq 0$. Express $\alpha(v) \in \mathcal{K}^2_\infty$ as $\alpha(v) = av^2$, $\beta(v,t) \in \mathcal{KL}^{1,e}_\infty$ as $\beta(v,t) = bve^{-\delta_1 t}$ and $\zeta \in \mathcal{L}^e$ as $\zeta(t) = ce^{-\delta_2 t}$ for some a, b, $c > 0$. Informally, boundedness follows from the fact that the globally exponentially stable "unperturbed" system $\dot{v} = -av^2$ has a higher order as $v \to \infty$ than the "perturbation" $bve^{-\delta_1 t} + ce^{-\delta_2 t}$. More in detail, in $\mathbb{R}_+$, for $v > 1$ it is $v < v^2$, hence we can write

$$bve^{-\delta_1 t} + ce^{-\delta_2 t} < (be^{-\delta_1 t} + ce^{-\delta_2 t})v \qquad \forall\, v > 1, \quad \forall\, t \geq t_o$$

or

$$\dot{v} < (-av + be^{-\delta_1 t} + ce^{-\delta_2 t})v \qquad \forall\, v > 1, \quad \forall\, t \geq t_o$$

meaning that for $v > \max\left(1, \frac{be^{-\delta_1 t_o} + ce^{-\delta_2 t_o}}{a}\right)$ it is $\dot{v} < 0$, $\forall\, t \geq t_o$, i.e., the solution of (A.1) remains bounded $\forall\, v_o \geq 0$ and $\forall\, t_o \geq 0$.

Furthermore, $\beta(v,t)$ and $\zeta(t)$ continuous, decreasing in t with $\beta(v,t) \to 0$ and $\zeta(t) \to 0$ as $t \to \infty$, imply also that for any $v_o > 0$ there exists a $t_1 \geq t_o$ such that $\forall\ t > t_1$ $\dot{v}(t) < 0$. Together with $\mathbb{R}_+$-invariance, this implies that $\lim_{t\to\infty} v(t) = d \geq 0$. To show that it must be $d=0$, let us assume by contradiction that $d>0$. Then

$$\lim_{t\to\infty}\dot{v}(t)=\lim_{t\to\infty}(-\alpha(v)+\beta(v,t)+\zeta(t))=-\alpha(d)<0,$$

meaning that there exists a $t_2>t_1$ and a $k\in(0,\ 1)$ such that

$$\dot{v}(t)<-k\alpha(d)<0 \qquad \forall\, t\geq t_2.$$

Applying the mean value theorem, we then have that $\exists\,\tau\in[t_2,\ t]$ such that

$$\frac{v(t)-v(t_2)}{t-t_2}=\dot{v}(\tau)<-k\alpha(d)<0 \qquad \forall\, t\geq t_2,$$

from which it follows

$$v(t)<-k\alpha(d)(t-t_2)+v(t_2)<0 \qquad \forall\, t\geq t_2,$$

which is a contradiction since $v\geq 0$. ■

With Lemma 1 in place, we can easily obtain the following sufficient condition for global convergence to the origin of a time-varying system in which the Lyapunov function has time derivative that is sign indefinite but bounded above by $\mathcal{KL}^{1,e}_{\infty}$ and $\mathcal{L}^e$ functions, i.e., by terms growing linearly in the norm of the state and decaying exponentially in time.

Lemma 2. *Assume that in the time-varying system (1) $g:\mathbb{R}_+\times\mathbb{R}^n\to\mathbb{R}^n$ is such that the solution of (1) exists unique in $[t_o,\infty)$ $\forall\, x_o\in\mathbb{R}^n$ and $\forall\, t_o\geq 0$. If there exists a continuously differentiable function $V(t,x):\mathbb{R}_+\times\mathbb{R}^n\to\mathbb{R}$, three $\alpha_1,\alpha_2,\alpha_3\in\mathcal{K}^2_{\infty}$, $\beta\in\mathcal{KL}^{1,e}_{\infty}$ and $\zeta\in\mathcal{L}^e$ such that*

$$\alpha_1(\|x\|)\leq V(t,x)\leq\alpha_2(\|x\|) \tag{A.2}$$

$$\frac{\partial V}{\partial t}+\frac{\partial V}{\partial x}g(t,x)\leq-\alpha_3(\|x\|)+\beta(\|x\|,t-t_o)+\zeta(t-t_o) \tag{A.3}$$

$\forall\, t\geq t_o$, $t_o\geq 0$ and $x_o\in\mathbb{R}^n$, then any solution of (1) converges to 0 uniformly in t_o as $t\to\infty$.

Proof. The right-hand side of (A.3) has the same structure as that of (A.1), meaning we can apply the comparison lemma, using (A.1) with initial condition $v(t_o)=V(t_o,x_o)$. Denoting $v(t)$ the corresponding solution, it is then

$$V(t,x)\leq v(t) \qquad \forall\, t\geq t_o. \tag{A.4}$$

From Lemma 1 and (A.4), it follows that for all x_o it must be $\lim_{t\to\infty}V(t,x(t))=0$ for any $t_o\geq 0$, hence from (A.2) $\lim_{t\to\infty}\alpha_1(x(t))=0$ or $\lim_{t\to\infty}x(t)=0$. ■

Remark 7. The sufficient conditions of Lemma 1 (and hence of Lemma 2) can be rendered more general using for instance the properties of input-to-state stability (Sontag & Wang, 1995), or of cascade nonlinear systems (Panteley & Loria, 2001).

Lemma 3. *For the output mask (11), it holds:*

$$\frac{\|y\|}{k}-\zeta(t)\leq\|x\|\leq\|y\|+\zeta(t) \tag{A.5}$$

where $k=\|I+\Phi\|$ and $\zeta(t)=\|e^{-\Delta t}\|\in\mathcal{L}^e$.

Proof. The inverse of (11) is

$$x=(I+\Phi e^{-\Sigma t})^{-1}y-e^{-\Delta t}\gamma \tag{A.6}$$

Notice that $\|I+\Phi e^{-\Sigma t}\|\leq\|I+\Phi\|=k$. We have from (11) and from the definition of $\zeta(t)$ that

$$\|y\|\leq k(\|x\|+\zeta(t)),$$

and from (A.6),

$$\|x\|\leq\|y\|+\zeta(t).$$

The bounds (A.5) follow combining these two inequalities. ■

A.2. Proof of Proposition 1

For (8) it is $\rho_i(x_{o,i})=|\gamma_i|$, hence it is enough that each agent chooses the parameter γ_i such that $|\gamma_i|>\lambda$, independently of $x_{o,i}$. For (9), $\rho_i(x_{o,i})=|(c_i-1)x_{o,i}+\gamma_i|>\lambda$ is satisfied for an infinite number of parameter pairs $(c_i,\ \gamma_i)$ with $c_i>1$ and $\gamma_i\neq 0$. When this inequality is satisfied for all agents then $\rho(x_o)>\lambda$. Similarly, for (10) there exist infinitely many parameter pairs $(\phi_i,\ \gamma_i)$ with $\phi_i>0$ and $\gamma_i\neq 0$ satisfying $\rho_i(x_{o,i})=|\phi_i x_{o,i}+(1+\phi_i)\gamma_i|>\lambda$. ■

A.3. Proof of Proposition 2

Proof. Consider an eavesdropping agent j trying to discern the initial condition of agent i, i.e., trying to estimate $x_{o,i}$ based on K1 and K2. This requires to compute the state of i from the available outputs. From (12), there are two possible ways to proceed. The first is to proceed "statically" by inverting $h_i(\cdot)$ in (12b), and the second to proceed dynamically using both (12a) and (12b). Concerning the first possibility, from (12b) computing $x_i(t,x_{o,i})$ from $y_i(t,x_{o,i})$ requires to invert the masked map $h_i(\cdot)$ for each t. From U1, however, this inversion is not possible for agent j, because $h_i(\cdot)$ is a privacy mask unknown to agent j. Concerning the second possibility, there are two possible options: the first is to use (12a) and (12b) to set up a system identification problem for $h_i(\cdot)$ and π_i. However, from Assumption 1, only a proper subset $\mathcal{M}_{ij}=\{\mathcal{N}_i\cup\{i\}\}\cap\{\mathcal{N}_j\cup\{j\}\}$ of all output trajectories entering into $f_i(\cdot)$ (i.e., $\{\mathcal{N}_i\cup\{i\}\}$) is available to agent j. Combining this with the essential neighborhood assumption (4), we obtain that agent j cannot correctly compute the right hand side of (12a), hence a system identification problem for (12) cannot be solved correctly. The second dynamical option is instead to consider the formal solution of (12a)

$$x_i(t)=x_{o,i}+\int_0^t f_i(y_i,\ y_k,\ k\in\mathcal{N}_i)d\tau.$$

Since $y^*=\lim_{t\to\infty}y(t)=\lim_{t\to\infty}x(t)=x^*$, if $i\in\mathcal{N}_j$, when $t\to\infty$, x_i^* is available to j, hence $x_{o,i}$ can be expressed as

$$x_{o,i}=x_i^*-\int_0^{\infty}f_i(y_i,\ y_k,\ k\in\mathcal{N}_i)d\tau. \tag{A.7}$$

Also in this case, however, Assumption 1 combined with the essential neighborhood assumption (4) implies that agent j cannot correctly estimate the integral in (A.7), as $\mathcal{M}_{ij}\nsubseteq\{\mathcal{N}_i\cup\{i\}\}$. In summary, since neither static nor dynamical methods for estimating $x_{o,i}$ can be applied, we can conclude that the initial condition $x_{o,i}$ is indiscernible for agent j. Since Assumption 1 is valid for all agents, we can also conclude that x_o is indiscernible, and therefore that (6) is a dynamically private version of (2). ■

A.4. Proof of Proposition 3

The right hand side of the dynamics in (6) is autonomous. Assume there exists y^* such that $f(y^*)=0$. Since, from P4 of Definition 3, $h(\cdot)$ is invertible in x for each t, by the implicit function theorem, there exists an $x^*(t)$ such that $y^*=h(t,x^*(t),\pi)$. If $x^*(t)$ is time-varying, then it is not an equilibrium point for (6). If instead x^* is time-invariant, then, from $\lim_{t\to\infty}y(t)=\lim_{t\to\infty}x(t)$, it must be $x^*=y^*$. But then, choosing $x(0)=x^*$, it is $y^*=h(0,x^*,\pi)=x^*$, i.e., P2 of Definition 3 is violated, hence also this case cannot happen in a privacy mask.

As for the second part, we need to show that $f(h(t,x,\pi))\to f(x)$ as $t\to\infty$ uniformly on compacts of $\mathbb{R}^n$ (Artstein, 1976). From P5 and $h\in C^1$, there exists an increasing, diverging sequence $\{t_k\}$ for which $h_i(t_k,x_i,\pi_i)\to x_i$ as $t_k\to\infty$, i.e., pointwise convergence holds. In particular, for any $\epsilon>0$, from pointwise convergence, there exists a $\nu_o(x_i)$ such that, for all $\nu > \nu_o$, $|h_i(t_\nu, x_i, \pi_i) - x_i| < \epsilon/2$. Pick two indexes $\nu_1 = \nu_1(x_i)$, $\nu_2 = \nu_2(x_i)$ such that $\nu_m > \nu_o$, $m = 1, 2$. Then $|h_i(t_{\nu_1}, x_i, \pi_i) - h_i(t_{\nu_2}, x_i, \pi_i)| \le |h_i(t_{\nu_1}, x_i, \pi_i) - x_i| + |h_i(t_{\nu_2}, x_i, \pi_i) - x_i| \le \epsilon/2 + \epsilon/2$. Selecting $\nu_s = \sup_{x_i \in \mathcal{X}_i} \{\nu_m(x_i),\ m = 1, 2\}$, then the Cauchy condition for uniform convergence applies and we have for any integer μ

$$|h_i(t_{\nu_s}, x_i, \pi_i) - x_i| = \lim_{\mu \to \infty} |h_i(t_{\nu_s}, x_i, \pi_i) - h_i(t_{\nu_s + \mu}, x_i, \pi_i)| \le \epsilon.$$

Hence, for a certain subsequence $\{t_\nu\}$ of $\{t_k\}$ it is $\sup_{x_i \in \mathcal{X}_i} |h_i(t_\nu, x_i, \pi_i) - x_i| \to 0$ as $k \to \infty$, meaning that for h_i convergence is uniform on compacts. Since f_i is Lipschitz continuous, it is uniformly continuous and bounded on compacts. Hence Lemma 1 of Lee et al. (2001) holds, and by a reasoning identical to the one above, if $\mathcal{X}$ is a compact of $\mathbb{R}^n$ we have:

$$\sup_{x \in \mathcal{X}} |f_i(h(t_\nu, x, \pi)) - f_i(x)| \to 0 \qquad \text{as} \quad \nu \to \infty.$$

The argument holds independently for any component f_i. Asymptotic time-independence and uniform convergence on compacts to $f(x)$ follow consequently. ∎

A.5. Proof of Theorem 1

By a standard converse theorem (e.g. Thm 4.14 of Khalil, 2002), global exponential stability of (2) with f globally Lipschitz implies ∃ a C^1 positive definite and radially unbounded Lyapunov function $V : \mathbb{R}^n \to \mathbb{R}_+$ and constants $b_i > 0$, $i = 1, \ldots, 4$, such that $\forall x \in \mathbb{R}^n$

$$b_1 \|x\|^2 \le V(x) \le b_2 \|x\|^2 \tag{A.8}$$

$$\frac{\partial V}{\partial x} f(x) \le -b_3 \|x\|^2 \tag{A.9}$$

$$\left\| \frac{\partial V}{\partial x} \right\| \le b_4 \|x\|. \tag{A.10}$$

With $y = C(x + e^{-\Delta t}\gamma)$, the system (6) can be rewritten as

$$\dot y = C\left(\dot x - \Delta e^{-\Delta t}\gamma\right) = Cf(y) - \begin{bmatrix} c_1 \delta_1 \gamma_1 e^{-\delta_1 t} \\ \vdots \\ c_n \delta_n \gamma_n e^{-\delta_n t} \end{bmatrix}. \tag{A.11}$$

Considering V evaluated in y, and computing its derivative along the trajectories of (A.11), we get:

$$\begin{aligned} \dot V &= \frac{\partial V}{\partial y} \dot y = \frac{\partial V}{\partial y} \left(\frac{\partial h}{\partial t} + \frac{\partial h}{\partial x} f(y) \right)_{x = h^{-1}(y)} \\ &= \frac{\partial V}{\partial y} Cf(y) - \frac{\partial V}{\partial y} C \Delta e^{-\Delta t} \gamma. \end{aligned} \tag{A.12}$$

Defining $k_1 = \|C\| > 0$, since (A.9) is valid everywhere, it is

$$\frac{\partial V}{\partial y} Cf(y) \le -k_1 b_3 \|y\|^2 = -\alpha(\|y\|),$$

for some $\alpha \in \mathcal{K}^2_\infty$, while the second term of (A.12) can be rewritten as

$$\frac{\partial V}{\partial y} C \Delta e^{-\Delta t} \gamma = \sum_i \frac{\partial V}{\partial y_i} c_i \delta_i \gamma_i e^{-\delta_i t}.$$

For each t, $c_i \delta_i \gamma_i e^{-\delta_i t} \le \zeta_1(t) \triangleq \max_i (c_i \delta_i |\gamma_i|) \max_i \left(e^{-\delta_i t}\right) \in \mathcal{L}^e$. Since

$$\frac{\partial V}{\partial y} = \frac{\partial V}{\partial x} \frac{\partial x}{\partial y} = \frac{\partial V}{\partial x} C^{-1},$$

from (A.10), Lemma 3 (where we impose $\sigma_i = 0$ and $c_i = 1 + \phi_i$) and $\|C^{-1}\| \le 1$, it is

$$\left\| \frac{\partial V}{\partial y} \right\| \le b_4 \|x\| \le b_4 \|y\| + \zeta_2(t)$$

for some $\zeta_2 \in \mathcal{L}^e$. Hence, for some constant $k_2 > 0$,

$$\begin{aligned} \frac{\partial V}{\partial y} C \Delta e^{-\Delta t} \gamma &\le k_2 b_4 \|y\| \zeta_1(t) + k_2 \zeta_1(t) \zeta_2(t) \\ &= \beta(\|y\|, t) + \zeta_3(t) \end{aligned}$$

with $\beta \in \mathcal{KL}^{1,e}_\infty$ and $\zeta_3 \in \mathcal{L}^e$. Therefore,

$$\dot V \le -\alpha(\|y\|) + \beta(\|y\|, t) + \zeta_3(t)$$

which has the same structure of (A.3), meaning that we can apply Lemma 2 and conclude that the system (2) is uniformly globally attracted to $x^* = 0$. Since (13) is a privacy mask, $\lim_{t \to \infty} y(t) = 0$ and Assumption 1 holds, from Proposition 2, (6) is a dynamically private version of (2). ∎

A.6. Proof of Corollary 1

Asymptotic autonomy of (A.11) is shown using an argument identical to that of the proof of Proposition 3. Convergence to the limit system $\dot y = Cf(y)$ and hence (14) follows consequently. From expression (A.11) it is also clear that, for all $y_o = h(0, x_o, \pi)$, $\Omega_{y_o} = \{0\}$, hence so it is for (6). ∎

A.7. Proof of Theorem 2

When $\Theta \neq 0$, $-(L + \Theta)$ is Hurwitz, as can be easily deduced from e.g. Chen et al. (2007). In the $z = x - x^*$ basis, for the unmasked system (16) a quadratic Lyapunov function can be used: $V(z) = z^T P z$, where $P = P^T > 0$ is the solution of the Lyapunov equation

$$P(L + \Theta) + (L + \Theta)^T P = Q$$

in correspondence of a given $Q = Q^T > 0$. The masked system (18) can be rewritten as

$$\begin{aligned} \dot x = &- (L + \Theta)\left(I + \Phi e^{-\Sigma t}\right) x \\ &- L\left(I + \Phi e^{-\Sigma t}\right) e^{-\Delta t} \gamma \\ &+ \Theta\left(I + \Phi e^{-\Sigma t}\right) x_o \end{aligned} \tag{A.13}$$

or, in z, after easy manipulations,

$$\begin{aligned} \dot z = &(L + \Theta)\left(I + \Phi e^{-\Sigma t}\right) z \\ &- L\left(I + \Phi e^{-\Sigma t}\right) e^{-\Delta t} \gamma \\ &+ \underbrace{(L + \Theta)\left[(L + \Theta)^{-1}\Theta,\ \left(I + \Phi e^{-\Sigma t}\right)\right]}_{\triangleq B(t)} x_o \end{aligned}$$

where $[\,\cdot\,,\,\cdot\,]$ is the matrix commutator. Notice that for this term we have $\|B(t)\| \le \zeta_1(t) \in \mathcal{L}^e$. Inserting $\dot z$ in $\dot V$:

$$\begin{aligned} \dot V = &- z^T \Big(P(L + \Theta)\left(I + \Phi e^{-\Sigma t}\right) \\ &\qquad + \left(I + \Phi e^{-\Sigma t}\right)(L + \Theta)^T P \Big) z \\ &+ 2 z^T \left(P(L + \Theta) B(t)\right) x_o \\ &- 2 z^T P L \left(I + \Phi e^{-\Sigma t}\right) e^{-\Delta t} \gamma. \end{aligned} \tag{A.14}$$

Looking at the terms of (A.14):

$$-z^T \Big(P(L + \Theta)\left(I + \Phi e^{-\Sigma t}\right) + \left(I + \Phi e^{-\Sigma t}\right)(L + \Theta)^T P \Big) z \le -\alpha_1(\|z\|), \tag{A.15}$$

$$2 z^T \left(P(L + \Theta) B(t)\right) x_o \le \alpha_2(\|z\|) \zeta_2(t), \tag{A.16}$$

$$-2 z^T P L \left(I + \Phi e^{-\Sigma t}\right) e^{-\Delta t} \gamma \le \alpha_3(\|z\|) \zeta_3(t), \tag{A.17}$$

where $\alpha_1 \in \mathcal{K}^2_\infty$, $\alpha_2, \alpha_3 \in \mathcal{K}^1_\infty$ and $\zeta_i \in \mathcal{L}^e$, meaning that $\beta_i(\|z\|, t) = \alpha_i(\|z\|)\zeta_i(t) \in \mathcal{KL}^{1,e}_\infty$, $i = 2, 3$. Therefore, overall we can write

$$\dot V \le -\alpha_1(\|z\|) + \beta(\|z\|, t)$$

where $\beta(\|z\|,t)=\max_{j=2,3}\alpha_j(\|z\|)\max_{j=2,3}\zeta_j(t)\in\mathcal{KL}_\infty^{1,e}$. Since V is quadratic, positive definite, radially unbounded and vanishing in $z=0$, there exist two class $\mathcal{K}_\infty^2$ functions α_4 and α_5 such that

$$\alpha_4(\|z\|)\le V(z)\le\alpha_5(\|z\|). \tag{A.18}$$

Hence we can apply Lemma 2 and obtain $\lim_{t\to\infty}z(t)=0$. In the original variables x, this implies $\lim_{t\to\infty}x(t)=x^*(x_o)$ for all x_o. Convergence of x to $x^*(x_o)$ is uniform in t because V does not depend on time. ■

A.8. Proof of Corollary 2

The first part follows from Proposition 3 and the second from $x^*(x_o)$ being a uniform attractor for each x_o. ■

A.9. Proof of Corollary 3

Same as proof of Corollary 2. ■

A.10. Proof of Theorem 4

Notice first that (24) implies the following one-sided global Lipschitz condition used in Yu et al. (2013):

$$(x-z)^T\big(f(x)-f(z)\big)\le q(x-z)^TR(x-z)\quad\forall\, x,\,z\in\mathbb{R}^\nu. \tag{A.19}$$

Denoting $e_i(t)=x_i(t)-s(t)$ the error of the i-th system from the desired trajectory, and using (28), then (26) can be written in terms of e_i as

$$\begin{aligned}\dot e_i &= f(y_i)-f(s)-\sum_{j=1}^n\ell_{ij}Re_j\\ &\quad-\sum_{j=1}^n\ell_{ij}R\Phi_je^{-\Sigma_jt}(e_j+s)\\ &\quad-\sum_{j=1}^n\ell_{ij}R\left(I+\Phi_je^{-\Sigma_jt}\right)e^{-\Delta_jt}\gamma_j\\ &\quad-p_iRe_i-p_iR\Phi_ie^{-\Sigma_it}(e_i+s)\\ &\quad-p_iR\left(I+\Phi_ie^{-\Sigma_it}\right)e^{-\Delta_it}\gamma_i.\end{aligned}$$

Denote $e=\begin{bmatrix}e_1^T & \dots e_n^T\end{bmatrix}^T$ and, for brevity, $\Psi_i(t)=I+\Phi_ie^{-\Sigma_it}$. A Lyapunov function, derived by that used in the standard pinned synchronization problem (Yu et al., 2013), is the following:

$$V(e,t)=\sum_{i=1}^n e_i^T\Psi_i(t)\xi_ie_i.$$

Since, for all t, $V(t,e)$ is quadratic, positive definite, vanishing at $e=0$, and radially unbounded, there exist two functions $\alpha_1,\ \alpha_2\in\mathcal{K}_\infty^2$ such that

$$\alpha_1(\|e\|)\le V(t,e)\le\alpha_2(\|e\|).$$

For its derivative along the trajectories of (26)–(28) it is:

$$\begin{aligned}\dot V(t,e) &= \frac{\partial V}{\partial e}\dot e+\frac{\partial V}{\partial t}\\ &= 2\sum_{i=1}^n e_i^T\Psi_i(t)\xi_i\dot e_i-\sum_{i=1}^n e_i^T\left(\Sigma_i\Phi_ie^{-\Sigma_it}\right)\xi_ie_i\\ &= 2\sum_{i=1}^n e_i^T\Psi_i(t)\xi_i\big(f(y_i)-f(s)\big) && \text{(A.20a)}\\ &\quad-2\sum_{i=1}^n e_i^T\Psi_i(t)\xi_i\sum_{j=1}^n\ell_{ij}R\Psi_j(t)e_j && \text{(A.20b)}\\ &\quad-2\sum_{i=1}^n e_i^T\Psi_i(t)\xi_i\sum_{j=1}^n\ell_{ij}R\Phi_je^{-\Sigma_jt}s && \text{(A.20c)}\\ &\quad-2\sum_{i=1}^n e_i^T\Psi_i(t)\xi_i\sum_{j=1}^n\ell_{ij}R\Psi_j(t)e^{-\Delta_jt}\gamma_j && \text{(A.20d)}\\ &\quad-2\sum_{i=1}^n e_i^T\Psi_i(t)\xi_ip_iR\Psi_i(t)e_i && \text{(A.20e)}\\ &\quad-2\sum_{i=1}^n e_i^T\Psi_i(t)\xi_ip_iR\Phi_ie^{-\Sigma_it}s && \text{(A.20f)}\\ &\quad-2\sum_{i=1}^n e_i^T\Psi_i(t)\xi_ip_iR\Psi_i(t)e^{-\Delta_it}\gamma_i && \text{(A.20g)}\\ &\quad-\sum_{i=1}^n e_i^T\left(\Sigma_i\Phi_ie^{-\Sigma_it}\right)\xi_ie_i. && \text{(A.20h)}\end{aligned}$$

Of the eight terms on the right hand side, the first is the most complicated and will be treated last. Three other are quadratic in $\|e\|$ and can be written as in Yu et al. (2013), using Kronecker products:

$$\text{(A.20b)}=-e^T\Psi(t)\Big((\Xi L+L^T\Xi)\otimes R\Big)\Psi(t)e$$

$$\text{(A.20e)}=-2e^T\Psi(t)\Big(\Xi P\otimes R\Big)\Psi(t)e$$

$$\text{(A.20h)}=-e^T\Sigma\Phi e^{-\Sigma t}\Xi\otimes Ie$$

where $\Psi=\mathrm{diag}(\Psi_1,\dots,\Psi_n)$, $\Sigma=\mathrm{diag}(\Sigma_1,\dots,\Sigma_n)$ and $\Phi=\mathrm{diag}(\Phi_1,\dots,\Phi_n)$. The remaining four are all linear in $\|e\|$ and decaying exponentially in t, and can be majorized in the following way

$$\begin{aligned}\text{(A.20c)} &\le k_1\|e\|\cdot\|(\Xi L+L^T\Xi)\otimes R\|\zeta_1(t)\\ &\le\beta_1(\|e\|,t)\end{aligned}$$

with $\zeta_1(t)=\max_{i,j}\Big\{\|\Psi_i(0)\|\cdot\big\|\Phi_j\big\|\cdot\|s(t)\|_\infty\Big\}\max_j\left\{e^{-\Sigma_jT}\right\}\in\mathcal{L}^e$ ($s(t)$ is bounded for all t), $k_1>0$, and $\beta_1\in\mathcal{KL}_\infty^{1,e}$;

$$\begin{aligned}\text{(A.20d)} &\le k_2\|e\|\cdot\|(\Xi L+L^T\Xi)\otimes R\|\zeta_2(t)\\ &\le\beta_2(\|e\|,t)\end{aligned}$$

$\zeta_2(t)=\max_j\left\{\|\Psi_i(0)\|\cdot\big\|\Psi_j(0)\gamma_j\big\|\right\}\max_j\left\{e^{-\Delta_jt}\right\}\in\mathcal{L}^e$, $k_2>0$, and $\beta_2\in\mathcal{KL}_\infty^{1,e}$;

$$\begin{aligned}\text{(A.20f)} &\le k_3\|e\|\cdot\|\Xi P\otimes R\|\zeta_1(t)\\ &\le\beta_3(\|e\|,t)\end{aligned}$$

$k_3>0$, $\beta_3\in\mathcal{KL}_\infty^{1,e}$;

$$\begin{aligned}\text{(A.20g)} &\le k_4\|e\|\cdot\|\Xi P\otimes R\|\zeta_2(t)\\ &\le\beta_4(\|e\|,t)\end{aligned}$$

$k_4>0$, $\beta_4\in\mathcal{KL}_\infty^{1,e}$. Finally for (A.20a), from (A.6),

$$\begin{aligned}e_i &= x_i-s=\underbrace{\left(I+\Phi_ie^{-\Sigma_it}\right)^{-1}}_{\triangleq F_i(t)}y_i-e^{-\Delta_i}\gamma_i-s\\ &= F_i(t)(y_i-s)+(F_i(t)-I)s-e^{-\Delta_i}\gamma_i\end{aligned}$$

where $F_i(t)$ is diagonal, positive definite, $\|F_i(t)\| \leq 1$, and $\lim_{t\to\infty} F_i(t) = I$. Hence

$$
\begin{aligned}
(A.20a) = {} & 2\sum_{i=1}^{n} (y_i - s)^T F_i(t)\Psi_i(t)\xi_i\big(f(y_i) - f(s)\big) \\
& + 2\sum_{i=1}^{n} \left(s^T(F_i(t) - I) - \gamma_i^T e^{-\Delta_i t}\right)\Psi_i(t)\xi_i\big(f(y_i) - f(s)\big) \\
& \leq 2\sum_{i=1}^{n} q(y_i - s)^T \Psi_i(t)F_i(t)\Psi_i(t)\xi_i R(y_i - s) \\
& \quad + \beta_5(\|y_i - \bar{s}\|,\ t) + \zeta_3(t)
\end{aligned}
$$

where for the first term we have used the one-sided Lipschitz condition

$$
\begin{aligned}
& (y_i - s)^T F_i(t)\Psi_i(t)\xi_i\big(f(y_i) - f(s)\big) \\
& \quad \leq q(y_i - s)^T F_i(t)\Psi_i(t)\xi_i R(y_i - s)
\end{aligned}
$$

which follows from (A.19) and the equivalence of norms, and for the second term the fact that, from (24), it depends linearly from $\|y - \bar{s}\|$ and it decays exponentially to 0 as $t \to \infty$, meaning that $\beta_5 \in \mathcal{KL}_\infty^{1,e}$ ($\bar{s}$ is the vector of n identical copies of s). Furthermore, since, from Lemma 3, $\|y - \bar{s}\| \leq k\|e\| + \zeta_4(t)$ for some $\zeta_4 \in \mathcal{L}^e$ and $k > 1$, it is $\beta_5(\|y - \bar{s}\|,\ t) \leq \beta_6(\|e\|,\ t) + \zeta_5(t)$ with $\beta_6 \in \mathcal{KL}_\infty^{1,e}$ and $\zeta_5 \in \mathcal{L}^e$. Inserting

$$
y_i - s = \Psi_i(t)e_i + \Phi_i e^{-\Sigma_i t}s + \Psi_i(t)e^{-\Delta_i t}\gamma_i
$$

and expanding, one gets a term quadratic in $\|e\|$,

$$
\sum_{i=1}^{n} q e_i^T \Psi_i(t)\xi_i R\Psi_i(t)e_i,
$$

plus several other terms of first or zero order in $\|e\|$, all vanishing exponentially fast in t. As long as $s(t)$ is bounded, using arguments identical to those above, we can therefore write

$$
(A.20a) \leq 2qe^T\Psi(t)\Xi \otimes R\Psi(t)e + \beta_7(\|e\|, t) + \zeta_6(t)
$$

with $\beta_7 \in \mathcal{KL}_\infty^{1,e}$ and $\zeta_6 \in \mathcal{L}^e$. Putting together all terms quadratic in $\|e\|$, since $\Psi(t)$ is diagonal positive definite and $\Sigma\Phi e^{-\Sigma t}\Xi \otimes I$ is positive definite for all t, it follows from (25) that there exists $\alpha_3 \in \mathcal{K}_\infty^2$ such that

$$
\begin{aligned}
& e^T\Psi(t)\left(2\,q\Xi \otimes R - 2\,\Xi P \otimes R - (\Xi L + L^T\Xi) \otimes R\right)\Psi(t)e \\
& - e^T\Sigma\Phi e^{-\Sigma t}\Xi \otimes Ie \leq -\alpha_3(\|e\|).
\end{aligned}
$$

Hence

$$
\dot{V} \leq -\alpha_3(\|e\|) + \beta(\|e\|, t) + \zeta(t)
$$

where $\beta(\|e\|, t) \in \mathcal{KL}_\infty^{1,e}$ majorizes $\beta_j(\|e\|, t)$, $j = 1, \ldots, 7$, and $\zeta(t) \in \mathcal{L}^e$ majorizes $\zeta_j(t)$, $j = 1, \ldots, 6$, meaning that we can apply the comparison lemma (Lemma 1), using (A.1) with initial condition $v(0) = V(0, e(0))$, and the result follows. ■

References

Aeyels, D., & Peuteman, J. (1998). A new asymptotic stability criterion for nonlinear time-variant differential equations. *IEEE Transactions on Automatic Control*, *43*(7), 968–971.

Alaeddini, A., Morgansen, K., & Mesbahi, M. (2017). Adaptive communication networks with privacy guarantees. In *2017 American control conference (ACC)* (pp. 4460–4465).

Altafini, C. (2019). A dynamical approach to privacy preserving average consensus. In *IEEE 58th conf. on decision and control*.

Ambrosin, M., Braca, P., Conti, M., & Lazzeretti, R. (2017). Odin: Obfuscation-based privacy-preserving consensus algorithm for decentralized information fusion in smart device networks. *ACM Transactions on Internet Technology*, *18*(1), 6:1–6:22.

Arcak, M., & Kokotovic, P. (2001). Observer-based control of systems with slope-restricted nonlinearities. *IEEE Transactions on Automatic Control*, *46*(7), 1146–1150.

Artstein, Z. (1976). Limiting equations and stability of nonautonomous ordinary differential equations. In J. LaSalle (Ed.), *CBMS regional conference series in applied mathematics*, *The stability of dynamical systems*. Philadelphia: SIAM.

Artstein, Z. (1977). The limiting equations of nonautonomous ordinary differential equations. *Journal of Differential Equations*, *25*(2), 184–202.

Astolfi, A. (2007). A remark on an example by teel & hespanha with applications to cascaded systems. *IEEE Transactions on Automatic Control*, *52*(2), 289–293.

Chaillet, A., & Angeli, D. (2008). Integral input to state stable systems in cascade. *Systems & Control Letters*, *57*(7), 519–527.

Chen, T., Liu, X., & Lu, W. (2007). Pinning complex networks by a single controller. *IEEE Transactions on Circuits and Systems. I. Regular Papers*, *54*(6), 1317–1326.

Cortés, J., Dullerud, G. E., Han, S., Ny, J. L., Mitra, S., & Pappas, G. J. (2016). Differential privacy in control and network systems. In *IEEE 55th conf. on decision and control* (pp. 4252–4272).

Duan, X., He, J., Cheng, P., Mo, Y., & Chen, J. (2015). Privacy preserving maximum consensus. In *2015 54th IEEE conference on decision and control (CDC)* (pp. 4517–4522).

Dwork, C. (2006). Differential privacy. In *Proceedings of the 33rd international conference on automata, languages and programming - Volume Part II, ICALP'06* (pp. 1–12). Berlin, Heidelberg: Springer-Verlag.

Farokhi, F., Shames, I., & Batterham, N. (2017). Secure and private control using semi-homomorphic encryption. *Control Engineering Practice*, *67*, 13–20.

Fontan, A., & Altafini, C. (2018). Multiequilibria analysis for a class of collective decision-making networked systems. *IEEE Transactions on Control of Networked Systems*, *5*(4), 1931–1940.

Gupta, N., Katz, J., & Chopra, N. (2017). Privacy in distributed average consensus. *IFAC-PapersOnLine*, *50*(1), 9515–9520, 20th IFAC World Congress.

Hale, M. T., & Egerstedt, M. (2017). Cloud-enabled differentially private multi-agent optimization with constraints. *IEEE Transactions on Control of Network Systems*, *PP*(99), 1.

He, J., Cai, L., Cheng, P., Pan, J., & Shi, L. (2019). Consensus-based data-privacy preserving data aggregation. *IEEE Transactions on Automatic Control*, 1.

Huang, Z., Mitra, S., & Dullerud, G. (2012). Differentially private iterative synchronous consensus. In *Proceedings of the 2012 ACM workshop on privacy in the electronic society, WPES '12* (pp. 81–90). New York, NY, USA: ACM.

Khalil, H. (2002). *Nonlinear systems* (3rd ed.). Pearson Education, Prentice Hall.

Kogiso, K., & Fujita, T. (2015). Cyber-security enhancement of networked control systems using homomorphic encryption. In *2015 54th IEEE conference on decision and control (CDC)* (pp. 6836–6843).

Lazzeretti, R., Horn, S., Braca, P., & Willett, P. (2014). Secure multi-party consensus gossip algorithms. In *2014 IEEE international conference on acoustics, speech and signal processing (ICASSP)* (pp. 7406–7410).

Lee, T.-C., Liaw, D.-C., & Chen, B.-S. (2001). A general invariance principle for nonlinear time-varying systems and its applications. *IEEE Transactions on Automatic Control*, *46*(12), 1989–1993.

Liu, Y., Wu, J., Manchester, I. R., & Shi, G. (2019). Dynamical privacy in distributed computing – part i: Privacy loss and PPSC mechanism. arXiv e-prints, arXiv:1902.06966.

Loria, A., Panteley, E., Popovic, D., & Teel, A. R. (2005). A nested matrosov theorem and persistency of excitation for uniform convergence in stable nonautonomous systems. *IEEE Transactions on Automatic Control*, *50*(2), 183–198.

Manitara, N. E., & Hadjicostis, C. N. (2013). Privacy-preserving asymptotic average consensus. In *2013 European control conference (ECC)* (pp. 760–765).

Markus, L. (1956). Asymptotically autonomous differential systems. In S. Lefschetz (Ed.), *Annals of mathematical studies*, *Contribution to the theory of nonlinear oscillations*. Princeton: Princeton Univ. Press.

Mo, Y., & Murray, R. M. (2017). Privacy preserving average consensus. *IEEE Transactions on Automatic Control*, *62*(2), 753–765.

Monshizadeh, N., & Tabuada, P. (2019). Plausible deniability as a notion of privacy. In *59th IEEE conference on decision and control (CDC)*.

Mu, X., & Cheng, D. (2005). On the stability and stabilization of time-varying nonlinear control systems. *Asian Journal of Control*, *7*(3), 244–255.

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

Ny, J. L., & Pappas, G. J. (2014). Differentially private filtering. *IEEE Transactions on Automatic Control*, *59*(2), 341–354.

Olfati-Saber, R., & Murray, R. (2004). Consensus problems in networks of agents with switching topology and time-delays. *IEEE Transactions on Automatic Control*, *49*(9), 1520–1533.

Panteley, E., & Loria, A. (1998). On global uniform asymptotic stability of nonlinear time-varying systems in cascade. *Systems & Control Letters*, *33*(2), 131–138.

Panteley, E., & Loria, A. (2001). Growth rate conditions for uniform asymptotic stability of cascaded time-varying systems. *Automatica*, *37*(3), 453–460.

Proskurnikov, A. V., & Tempo, R. (2017). A tutorial on modeling and analysis of dynamic social networks. part i. *Annual Reviews in Control*, *43*, 65–79.
Rezazadeh, N., & Kia, S. (2018). Privacy preservation in a continuous-time static average consensus algorithm over directed graphs. In *American control conference* (pp. 5890–5895).
Rouche, N., Habets, P., & Laloy, M. (2012). *Applied mathematical sciences*, *Stability theory by liapunov's direct method*. Springer New York.
Ruan, M., Gao, H., & Wang, Y. (2019). Secure and privacy-preserving consensus. *IEEE Transactions on Automatic Control*, *64*(10), 4035–4049.
Saberi, A., Kokotovic, P., & Sussmann, H. (1990). Global stabilization of partially linear composite systems. *SIAM Journal on Control and Optimization*, *28*(6), 1491–1503.
Sontag, E. D. (2003). A remark on the converging-input converging-state property. *IEEE Transactions on Automatic Control*, *48*(2), 313–314.
Sontag, E. D., & Krichman, M. (2003). An example of a GAS system which can be destabilized by an integrable perturbation. *IEEE Transactions on Automatic Control*, *48*(6), 1046–1049.
Sontag, E. D., & Wang, Y. (1995). On characterizations of the input-to-state stability property. *Systems & Control Letters*, *24*(5), 351–359.
Sussmann, H. J., & Kokotovic, P. V. (1991). The peaking phenomenon and the global stabilization of nonlinear systems. *IEEE Transactions on Automatic Control*, *36*(4), 424–440.
Teel, A. R., & Hespanha, J. (2004). Examples of GES systems that can be driven to infinity by arbitrarily small additive decaying exponentials. *IEEE Transactions on Automatic Control*, *49*(8), 1407–1410.
Wiese, M., Johansson, K. H., Oechtering, T. J., Papadimitratos, P., Sandberg, H., & Skoglund, M. (2016). Secure estimation for unstable systems. In: *Proc. IEEE 55th conf. dec. contr. (CDC)* (pp. 5059–5064).
Yu, W., Chen, G., Lü, J., & Kurths, J. (2013). Synchronization via pinning control on general complex networks. *SIAM Journal on Control and Optimization*, *51*(2), 1395–1416.
Zhou, J., an Lu, J., & Lü, J. (2008). Pinning adaptive synchronization of a general complex dynamical network. *Automatica*, *44*(4), 996–1003.

Claudio Altafini received a Master degree ("Laurea") in Electrical Engineering from the University of Padova, Italy, in 1996 and a Ph.D. in Optimization and Systems Theory from the Royal Institute of Technology, Stockholm, Sweden in 2001. From 2001 till 2013 he was with the International School for Advanced Studies (SISSA) in Trieste, Italy. Since 2014 he is a Professor in the Division of Automatic Control, Dept. of Electrical Engineering at Linkoping University, Sweden. He is a past Associate Editor for the IEEE Trans. on Automatic Control (2013-15) and he is currently serving as Associate Editor for the IEEE Trans. on Control of Network Systems and Automatica. His research interests are in the areas of nonlinear systems analysis and control, with applications to quantum mechanics, systems biology and complex networks.