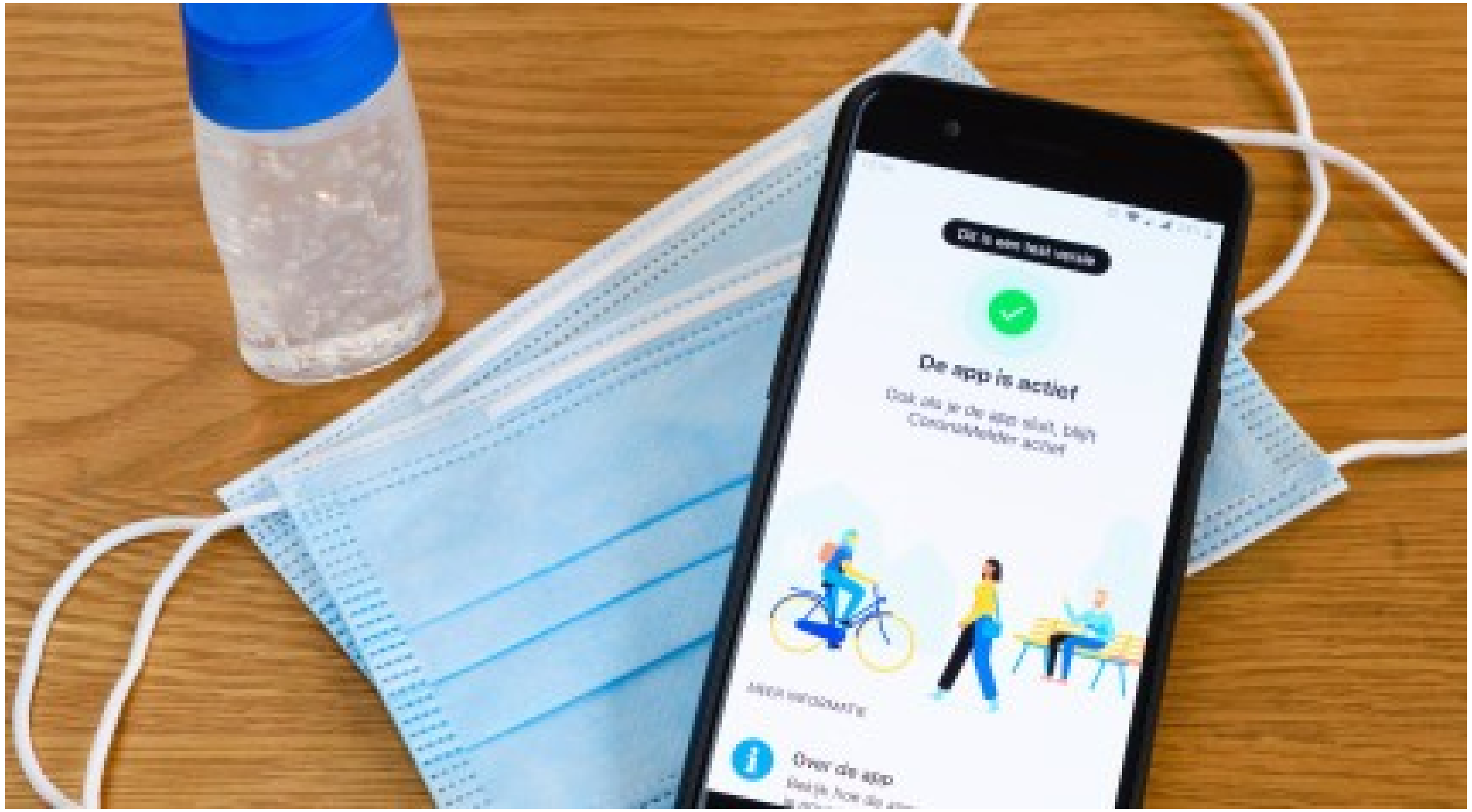
Privacy-preserving dynamic controllers

Ming Cao

Engineering and Technology Institute
University of Groningen
The Netherlands

Yu Kawano, Hiroshima University, Japan



COVID-19 Contact Tracing Apps

The apps have been designed with privacy as a crucial priority:

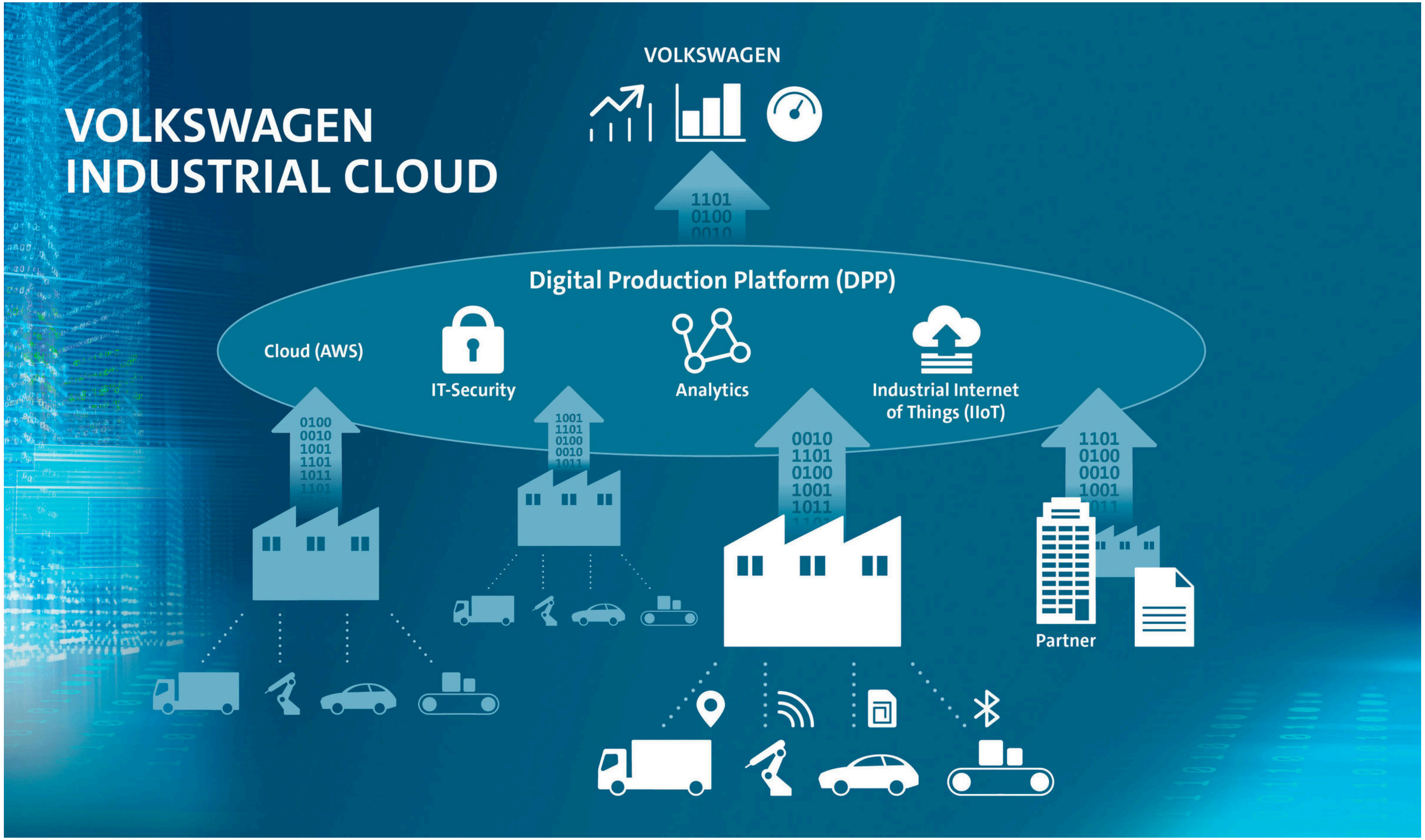
- ✓ Not using GPS location or tracking
- ✓ Not checking whether self-isolating
- ✓ Not used by law enforcement
- ✓ Not to collect personal information on the phone

Privacy fears still stop most people using COVID contact tracing apps.

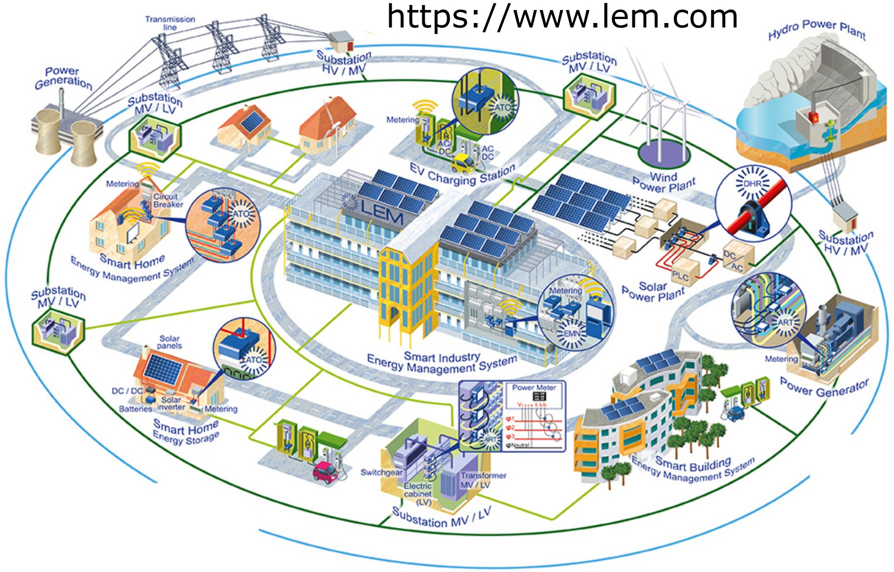
“Game-theoretic modeling of collective decision making during epidemics”, *Physical Review E*, 2021.

“Collective patterns of social diffusion are shaped by individual inertia and trend seeking”, *Nature Communications*, 2021.

Privacy is also of central importance for industrial data!



Privacy of Dynamical Systems



https://www.lem.com

Smart Grid

- In traditional computer science, privacy analysis of static data
- In IoT technologies, a lot of data are generatied by dynamical systems

⬇

Privacy of dynamical systems?

<u>Fundamental Questions</u>

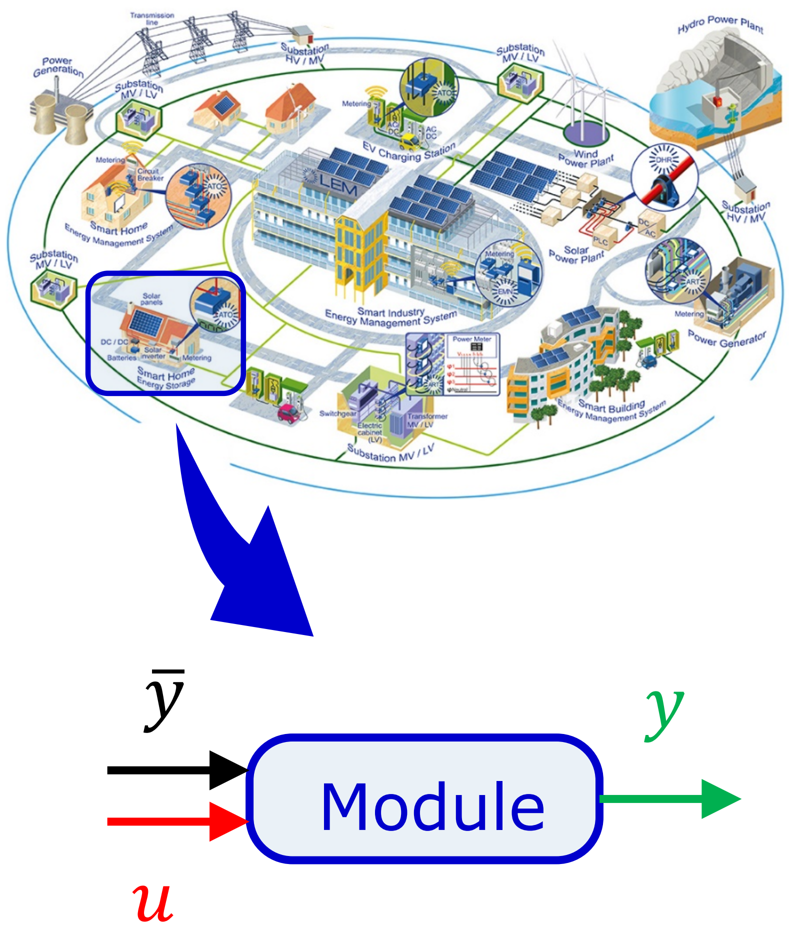
- How to anlayze privacy with tools of systems and conrol?
- Can we design a controller while addresing privacy concern?

Outline

- Differential privacy and input observability

- Control design while addressing privacy concern
  - Centralized tracking control
  - Decentralized tracking control and foundamental trade-off

Privacy Analysis of Each Module



- Dynamics of a module

$$x(t+1) = Ax(t) + Bu(t), \quad x(0) = x_0$$
$$y(t) = Cx(t) + Du(t)$$

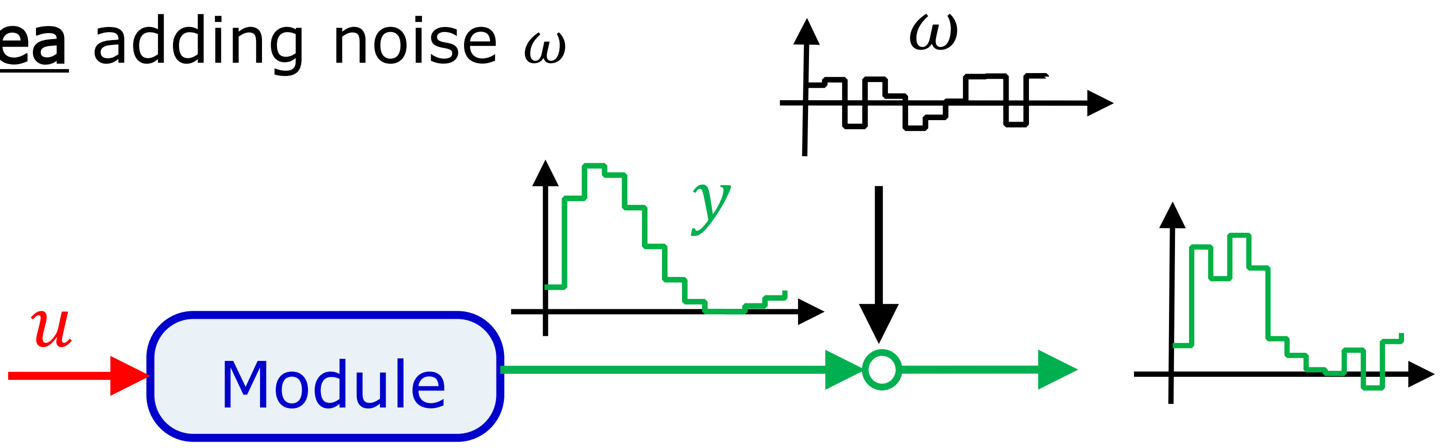
$u(t) \in \mathbb{R}^m$: own input of the module
$y(t) \in \mathbb{R}^p$: published signal

Question

How to protect u (and x_0) from being inferred from y?

Idea for Private Data Protection

Idea adding noise ω



$y + \omega$ is sensed by other modules

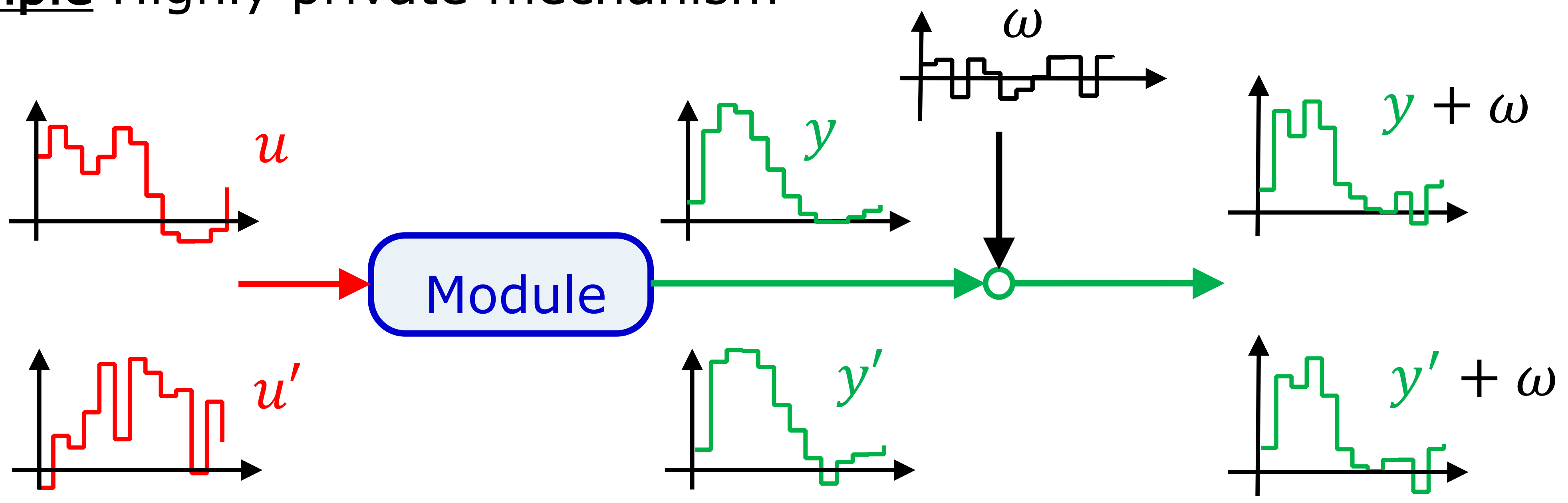
Problem

Design ω such that u is difficult to estimate from $y + \omega$ in a certain privacy level

- Problem depends on dynamics of module: Input Observability
- Criterion of privacy: Differential Privacy [Dwork et al, ICALP:06 Le Ny, Pappas, TAC:13]

Privacy: comparing pairs of outputs

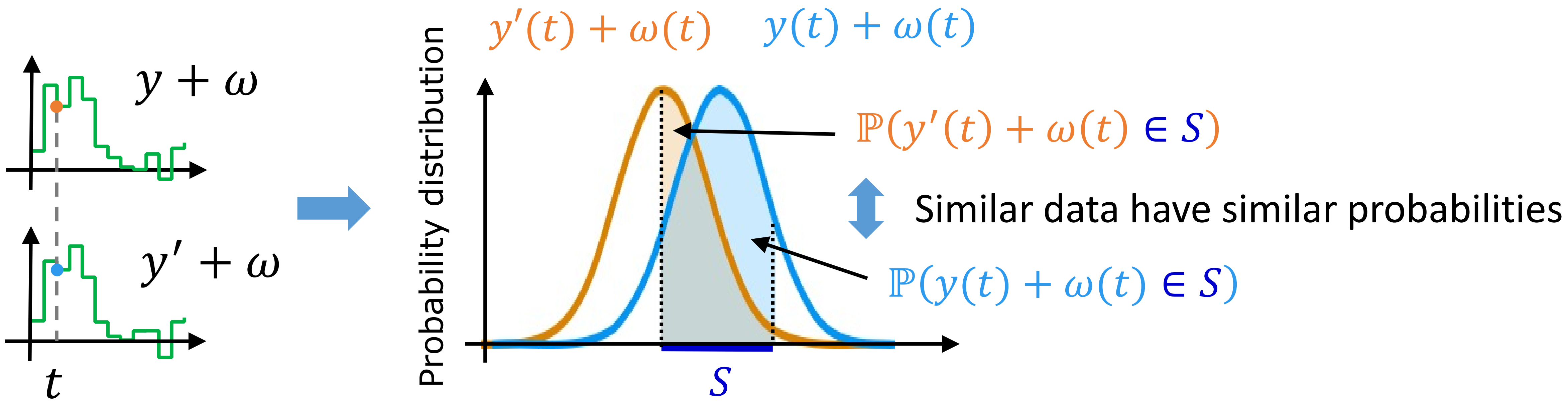
<u>Example</u> Highly private mechanism



If for any input pair (u, u'), output pair $(y + \omega, y' + \omega)$ is similar then the input is difficult to be estimated from the output

Differential Privacy at a Time Instant

time instant $\boldsymbol{k}$



Small imply similar distributions

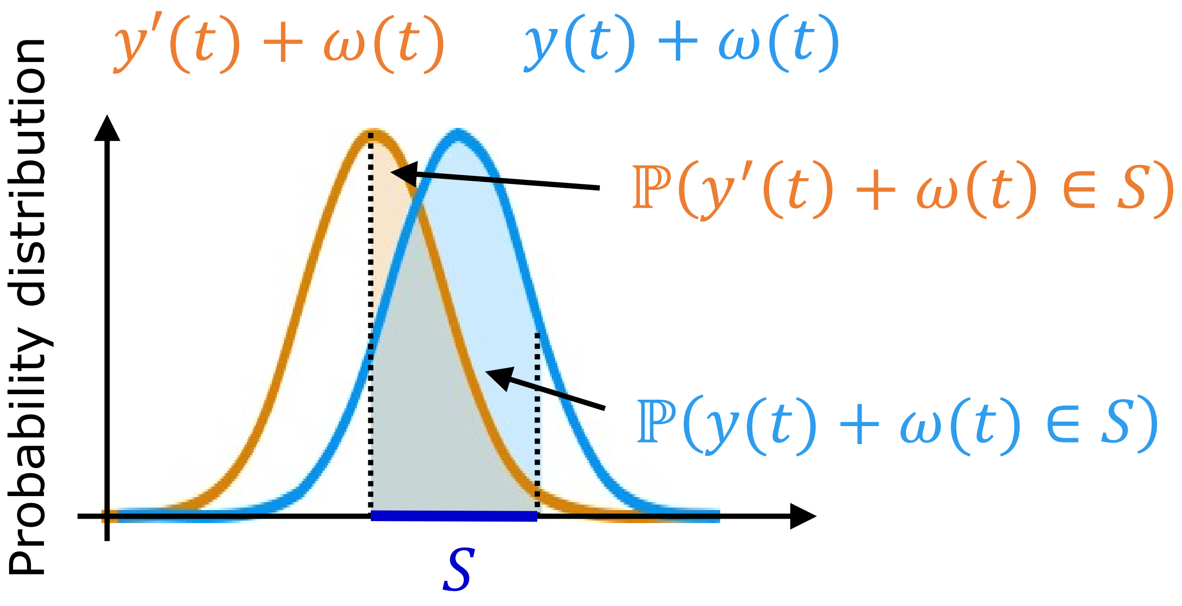
[Def] $(\boldsymbol{\varepsilon}, \boldsymbol{\delta})$-differential privacy $(\varepsilon, \delta \geq 0)$

$$\mathbb{P}(y(t) + \omega(t) \in S) \leq e^{\varepsilon} \mathbb{P}(y'(t) + \omega(t) \in S) + \delta \quad \forall S$$

Roles of ε and δ

[Def] <u>$(\boldsymbol{\varepsilon}, \boldsymbol{\delta})$-differential privacy</u> $(\varepsilon, \delta \geq 0)$

$$\mathbb{P}(y(t) + \omega(t) \in S) \leq e^{\varepsilon}\, \mathbb{P}(y'(t) + \omega(t) \in S) + \delta \quad \forall S$$



When $\delta = 0$, $\mathbf{log}_{\boldsymbol{e}}$**-distance**

$$\log_e \mathbb{P}(y'(t) + \omega(t) \in S) - \log_e \mathbb{P}(y(t) + \omega(t) \in S) = \log_e \frac{\mathbb{P}(y'(t) + \omega(t) \in S)}{\mathbb{P}(y(t) + \omega(t) \in S)} \leq \varepsilon$$

<u>$(\boldsymbol{\varepsilon}, \boldsymbol{\delta})$-differential priacy</u>

➡ $(2\varepsilon, 0)$-differential priacy with probability $1 - \frac{2\delta}{\varepsilon\, e^{\varepsilon}}$

Differential Privacy of Dynamical Systems

Signals

$$U_t = \begin{bmatrix} u(0) \\ \vdots \\ u(t) \end{bmatrix} \in \mathbb{R}^{m(t+1)}, \quad Y_t = \begin{bmatrix} y(0) \\ \vdots \\ y(t) \end{bmatrix} \in \mathbb{R}^{p(t+1)}, \quad \Omega_t = \begin{bmatrix} \omega(0) \\ \vdots \\ \omega(t) \end{bmatrix} \in \mathbb{R}^{m(t+1)}$$

[Def] **(ε, δ)-differential privacy at time t** $(\varepsilon, \delta, t, c \geq 0)$

$$\mathbb{P}(Y_t + \Omega_t \in S) \leq e^{\varepsilon} \mathbb{P}(Y_t' + \Omega_t \in S) + \delta \quad \forall S \subset \mathbb{R}^{p(t+1)}$$

for all $|(x_0, U_t) - (x_0', U_t')|_2 \leq c$

Similarity of input data (2-norm)

- Privacy criterion for (x_0, U_t)
- Small (ε, δ) imply high privacy

$$Y_t = \underbrace{\begin{bmatrix} C \\ CA \\ \vdots \\ CA^t \end{bmatrix}}_{=: O_t} x_0 + \underbrace{\begin{bmatrix} D & 0 & \cdots & 0 \\ CB & \ddots & \ddots & \vdots \\ \vdots & \ddots & D & 0 \\ CA^{t-1}B & \cdots & CB & D \end{bmatrix}}_{=: N_t} U_t$$

Noise Design for Differential Privacy

- Multivariate Gaussian noise $\Omega_t \sim \mathcal{N}(0, \Sigma)$

> [Thm] Given $\varepsilon > 0$ and $1/2 > \delta > 0$, the system is (ε, δ)-differentially private at a finite time t if
>
> $$\lambda_{\max}^{-\frac{1}{2}}([O_t \quad N_t]^\top \Sigma^{-1} [O_t \quad N_t]) \geq c\mathrm{R}(\varepsilon, \delta)$$

$$\mathrm{R}(\varepsilon, \delta) := Q^{-1}(\delta) + \sqrt{\left(Q^{-1}(\delta)\right)^2 + 2\varepsilon} / 2\varepsilon, \quad \mathrm{Q}(w) := \frac{1}{\sqrt{2\pi}} \int_w^\infty e^{-\frac{v^2}{2}} dv, \quad Y_t = O_t x_0 + N_t U_t$$

- LHS can be made arbitrary large by choosing variance Σ larege
- Condition depends on system dynamics $[O_t \quad N_t]$

Variations of Differential Privacy Conditions

- i.i.d. Gaussian case: $\omega(t) \sim \mathcal{N}(0, \sigma)$

$$\sigma \geq \lambda_{\max}^{1/2}([O_t \quad N_t]^\top [O_t \quad N_t]) c\mathrm{R}(\varepsilon, \delta)$$

- For a stable system, condition for any $t \geq 0$:

$$\sigma \geq \left(\lambda_{\max}^{1/2}(\mathcal{O}_\infty) + \gamma\right) c\mathrm{R}(\varepsilon, \delta)$$

$\mathcal{O}_\infty$: observability Gamian
γ: H_∞-norm

- i.i.d Laplace noise: $\omega(t) \sim \mathrm{Lap}(0, 2b^2)$

$(\varepsilon, 0)$-differential privacy at a finite time t if

$$b \geq c||[O_t \quad N_t]||_1 / \varepsilon$$

Outline

- Differential privacy and input observability
- Control design while addressing privacy concern
  - Centralized tracking control
  - Decentralized tracking control and foundamental trade-off

Strong Input Observability

[Def] <u>**Strong input observability**</u>

There exists a finite time T such that $(x_0, u(0))$ is uniquely determined from Y_t

Strong input observability

$\Rightarrow$ $(x(1), u(1))$ is constructed from Y_{t+1}

$\Rightarrow$ $u(0), u(1), \ldots$ are determined recursively

Specific strong input observability

If $u(0), u(1), \ldots$ are known, standard observability

If x_0 is known, input observability (left invertibility)

Least Square Estimation of (x_0, U_t)

Problem Measured $Y_t + \Omega_t$ with i.i.d. Ω_t, $\min_{(x_0,U_t)} |(Y_t + \Omega_t) - (O_t x_0 + N_t U_t)|_2^2$

Solution $[O_t \quad N_t]^\top [O_t \quad N_t] \begin{bmatrix} x_0^* \\ U_t^* \end{bmatrix} = [O_t \quad N_t]^\top (Y_t + \Omega_t)$

[Def] **Strong input observability Gramian**: $[O_t \quad N_t]^\top [O_t \quad N_t]$

Quality: Strongly input observability $\Leftrightarrow$ Nonsingularity of the Gramian

Quantity: All eigenvalues are large
$\Rightarrow$ highly input observable i.e. less private

Differential privacy condition: $\sigma \geq \lambda_{\max}^{1/2}([O_t \quad N_t]^\top [O_t \quad N_t]) c\mathrm{R}(\varepsilon, \delta)$

Observations from Gramian

- $\lambda_{\max}([O_t \quad N_t]^\top [O_t \quad N_t])$ is non-decreasing w.r.t t

  ➡ More data are being collected, less private a system becomes

- ith $m \times m$ block diagonal element of $N_t^\top N_t$:

$$(N_t^\top N_t)_{i,i} := D^\top D + \sum_{k=0}^{t-i} \left(CA^k B\right)^\top \left(CA^k B\right), i = 1,2,\ldots,t$$

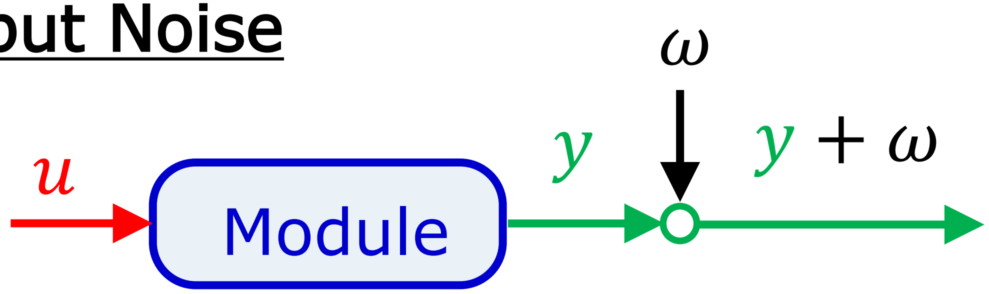
  This is the Gramian corresponding to the initial input $u(0)$, and
  $\mathrm{trace}(N_t^\top N_t) = \mathrm{trace}(N_t^\top N_t)_{1,1} + \cdots + \mathrm{trace}(N_t^\top N_t)_{t,t}$

  ➡ If $(x_0, u(0))$ is easy to estimate, so is (x_0, U_t).

- Detailed privacy analysis is doable by using subspaces corresponding to eingevalues of $[O_t \quad N_t]^\top [O_t \quad N_t]$

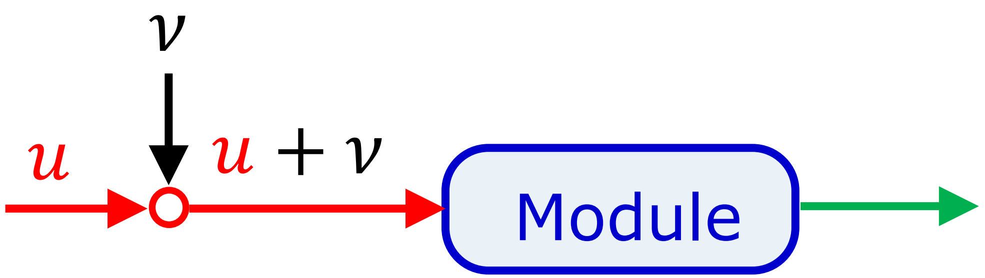
Remark: Input Noise vs Output Noise

Output Noise



- Differential privacy level depends on $[O_t \; N_t]$ and w
- Data utility depends on w

Input Noise



- Differential privacy level depends on only ν
- Data utility depends on $[O_t \; N_t]$ and ν

The same differential privacy levels can be achieved

Summary of Differential Privacy Analysis

- Privacy criterion of (x_0, U_t): $(\boldsymbol{\varepsilon}, \boldsymbol{\delta})$**-differential privacy**

$$\mathbb{P}(Y_t + \Omega_t \in S) \leq \mathrm{e}^{\varepsilon}\mathbb{P}(Y_t' + \Omega_t \in S) + \delta\,, \quad Y_t = O_t x_0 + N_t U_t$$

  Small $\varepsilon, \delta \geq 0$ mean higher privacy

- For i.i.d. $\omega(t) \sim \mathcal{N}(0, \sigma)$, the system is (ε, δ)-differentially private if

$$\sigma \geq \lambda_{\max}^{\frac{1}{2}}([O_t \quad N_t]^\top [O_t \quad N_t]) c\mathrm{R}(\varepsilon, \delta)$$

strong input observability Gramian

- System is highly strongly input observable
  ⇒ Large noise is needed to increase the privacy level

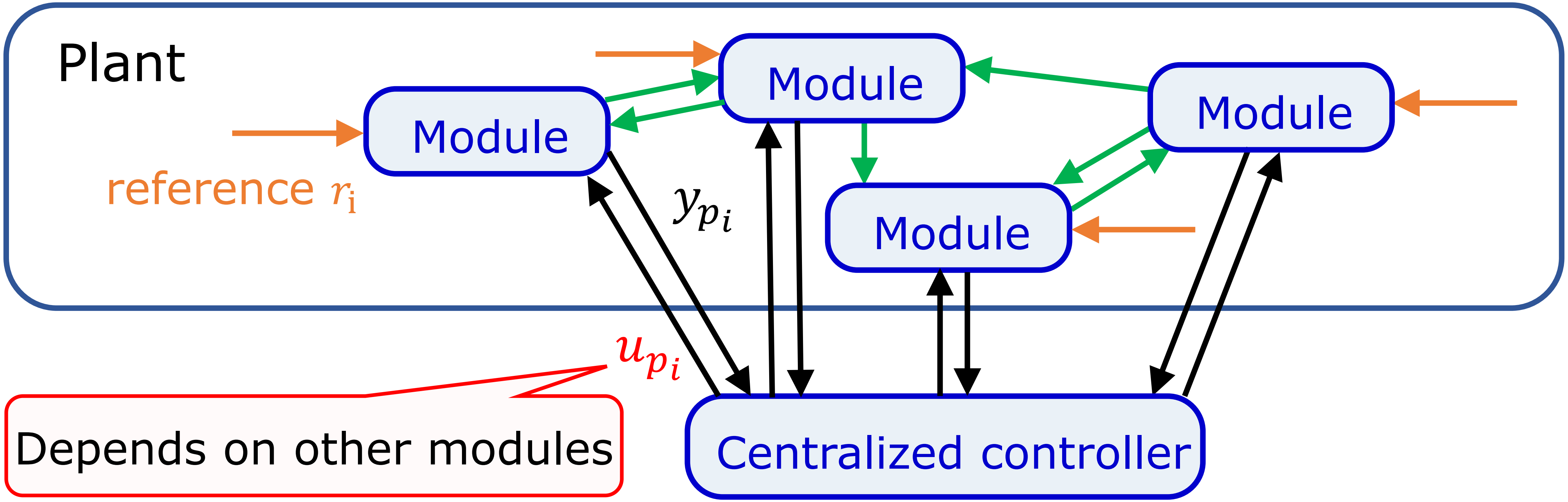
- Similar observation for non-i.i.d. case and even for nonlinear systems

Outline

- Differential privacy and input observability

- Control design while addressing privacy concern
  - ➢ Centralized tracking control
  - ➢ Decentralized tracking control and foundamental trade-off

Problem Formulation



y_p: output, r: reference
u_p: input

Control objective $\lim_{t\to\infty} \left(y_p(t) - r(t)\right) = 0$

Privacy concern Private info. (as y_{pi}, r_i) of modules are infered from u_{pj}

Tracking Control: Standard Assumptions

Plant

$$x_p(t+1) = A_p x_P(t) + B_p u_p(t)$$
$$y_p(t) = C_p x_p(t) + D_p u_p(t)$$

Reference generator

$$x_r(t+1) = A_r x_r(t)$$
$$r(t) = C_r x_r(t)$$

Assumptions

1. A_r is not Schur stable
2. (A_p, B_p) is stabilizable
3. $\left(\begin{bmatrix} C_p & -C_r \end{bmatrix}, \begin{bmatrix} A_p & 0 \\ 0 & A_r \end{bmatrix}\right)$ is stabilizable
4. The Sylvester equation has a pair of solutions (X, U)

$$XA_r = A_p X + B_P U$$
$$0 = C_p X + D_p U - C_r$$

Standard Tracking Controller and Privacy

Design parameters: G_1, L

Standard tracking controller

$$u_p(t) = [G_1 \quad G_2]x_c(t)$$

$$x_c(t+1) = \left(\begin{bmatrix} A_p & 0 \\ 0 & A_r \end{bmatrix} + L[C_p \quad -C_r] + \left(\begin{bmatrix} B_p \\ 0 \end{bmatrix} + LD_p\right)[G_1 \quad G_2]\right)x_c(t)$$
$$-L\left(y_p(t) - r(t)\right)$$

Conditions

Stabilization: $A_p + B_p G_1$ and $\begin{bmatrix} A_p & 0 \\ 0 & A_r \end{bmatrix} + L[C_p \quad -C_r]$ are Schur stable

Tracking: $G_2 = U - G_1 X$

Privacy requirment

Estimating y_p from u_p is difficult

inputs of controller (y_p) outputs of controller (u_p)

➡ Privacy analysis of controller dynamics

Storagegy for Privacy-protection

Ideal: Private inf. contained in y_p and r belong to input unobservable subspace ➡ NP hard

Differential privacy condition of stable system for any $t \geq 0$:

$\sigma \geq \gamma c \mathrm{R}(\varepsilon, \delta)$ γ: H_∞-norm $\omega(t) \sim \mathcal{N}(\mu, \sigma)$

Strategy for privacy-protection

Design a tracking controller having a small H_∞-norm

Both tracking controller and closed-loop system need to be Schur stable

➡ Strong stabilization problem

Negative Result for Strong Stabilization

Plant

$$x_p(t+1) = A_p x_P(t) + B_p u_p(t)$$
$$y_p(t) = C_p x_p(t) + D_p u_p(t)$$

Reference

$$x_r(t+1) = A_r x_r(t)$$
$$r(t) = C_r x_r(t)$$

[Thm] If $D_p = 0$, the tracking controller cannot be Schur stable

Standard tracking controller with $D_p = 0$

$$u_p(t) = [G_1 \quad G_2] x_c(t)$$
$$x_c(t+1) = \left(\begin{bmatrix} A_p & 0 \\ 0 & A_r \end{bmatrix} + L[C_p \quad -C_r] + \begin{bmatrix} B_p \\ 0 \end{bmatrix} [G_1 \quad G_2] \right) x_c(t) - L\left(y_p(t) - r(t)\right)$$

A_r is not Schur stable (Assumption 1) nor stabilizable (by PBH test)

A_r does not appear if we use x_r directly

Proposed Tracking controller

<u>Proposed tracking controller</u>

Design parameters: G_1, L

$$u_p(t) = G_1 x_c(t) + G_2 x_r(t)$$
$$x_c(t+1) = \left(A_p + \left(B_p + LD_p\right)G_1 + LC_p\right)x_c(t) + \left(B_p + LD_p\right)G_2 x_r(t) - L y_p(t)$$

<u>Conditions for tracking</u>

Stabilization: $A_p + B_p G_1$ and $A_p + LC_p$ are Schur stable

Tracking: $G_2 = U - G_1 X$

<u>Privacy requirement</u>

Protecting $x_r(t)$ is also doable

H_∞-norm of the controller from y_p to u_p is small

➡ Privacy-preserving control design is formulated as a *strong stabilization problem*

Privacy-preserving Dynamic Controller

<u>**Design procedure by LMIs**</u>

For finding G_1, L simultaneously we need to solve BMI

1. Find G_1 stabilizing $A_p + B_p G_1$

2. Find $L := P^{-1}\hat{L}$ by solving

$$\begin{bmatrix} P & * \\ (PA_p + \hat{L}C_p)^\top & P \end{bmatrix} > 0 \iff \text{Stability of } A_p + L\,C_p$$

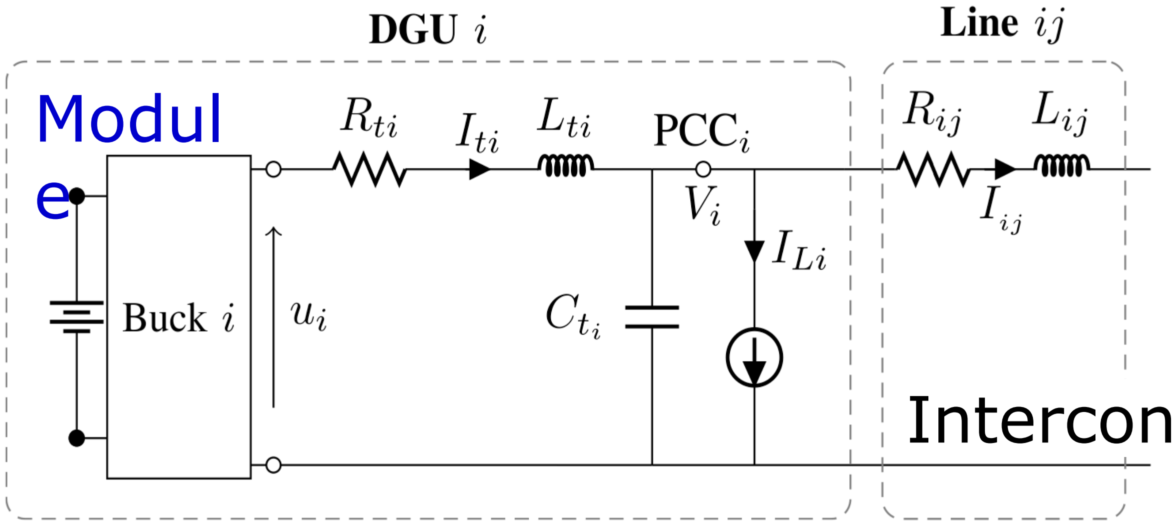
$$\begin{bmatrix} P & * & * & * \\ 0 & \gamma^2 I & * & * \\ P(A_p + B_p G_1) + \hat{L}(C_p + D_p G_1) & -\hat{L} & P & * \\ G_1 & 0 & 0 & I \end{bmatrix} > 0$$

$\iff$ H_∞-norm from y_p to u_p is less than γ

γ is designed based on
$\sigma \geq \gamma c \mathrm{R}(\varepsilon, \delta)$
$\omega \sim \mathcal{N}(0, \sigma)$

3. Designed control input: $u_p + \omega$

Example: DC Microgrids



$I_{L,i}$: load current (demand, const)

$I_{T,i}$: generator current (supply)

$I_{i,j}$: current between i and j

V_i: load voltage

$$L_i \dot{I}_i = -R_i I_i - V_i + u_i$$

$$C_i \dot{V}_i = I_i - I_{L,i} - \sum_{j \in N_i} I_{i,j}$$

$$L_{i,j} \dot{I}_{i,j} = V_i - V_j - R_{i,j} I_{i,j}$$

$$y_{i,1} = V_i,\ y_{i,2} = I_i$$

Control objective

$$\lim_{t\to\infty} I_i(t) = L_{L,i} \qquad \lim_{t\to\infty} V_i(t) = V^*$$

Private info. against others: $I_{T,i}$

Example: DC Microgrids (Scenario)

Sampling period for descritization: $10^{-3}[s]$

Physical parameters
[Cucuzzella et al., IEEE TCST: 19]

$N = 2$ (2 user)
$R_i = 0.2[\Omega]$
$R_{i,j} = 70[\mathrm{m}\Omega]$
$L_i = 1.8[\mathrm{mH}]$
$C_i = 2.2[\mathrm{mF}]$
$V^* = 380[\mathrm{V}]$

Control objective

$$\lim_{t\to\infty} I_i(t) = 0 \qquad \lim_{t\to\infty} V_i(t) = V^*$$

Reference generator

$$x_r(t+1) = x_r(t)$$
$$y_r(t) = x_r(t)$$

Scenario

User 1 starts to use more electricity

Initial conditions

$I_1(0) = -4[A],\ I_2(0) = 0[A]$
$I_{1,2}(0) = 0[A],\ V_i(0) = 380[V], i = 1,2$

Privacy-preserving Tracking Controller

Computing G_1 based on optimal control: $J = \sum_{t=0}^{\infty} |x_p(t)|^2 + |u_p(t)|^2$

$$G_1 = \begin{bmatrix} -0.85 & 0.037 & -0.461 & -0.007 & 0.229 \\ 0.037 & -0.85 & -0.007 & -0.461 & -0.229 \end{bmatrix}$$

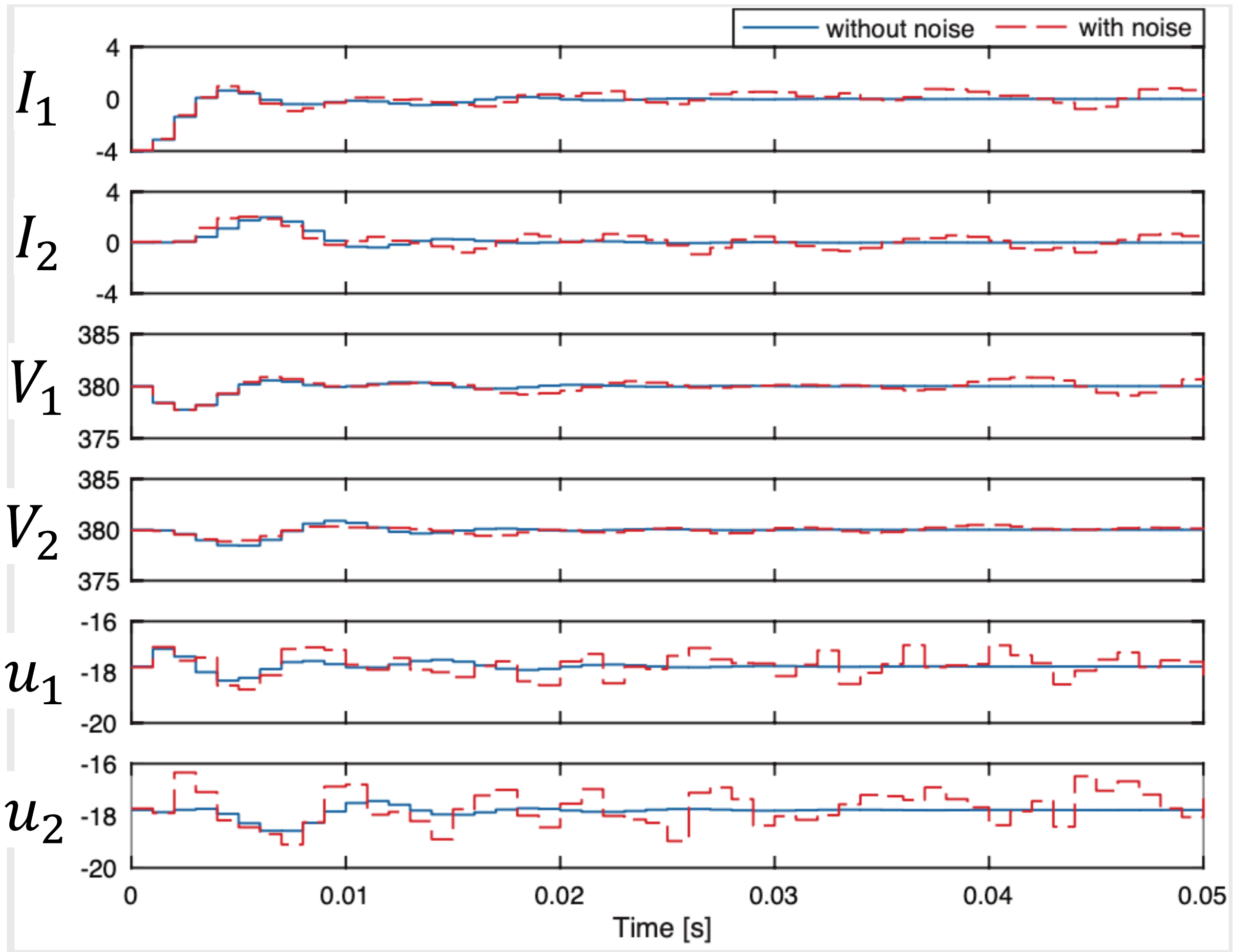
Finding L based on LMIs for $\gamma = 0.365$

$$L = \begin{bmatrix} -0.193 & 0.0088 & 0.0828 & 0.0111 \\ 0.0088 & -0.193 & 0.0111 & 0.0828 \\ -0.0717 & 0.0072 & -0.134 & -0.0129 \\ 0.0072 & -0.0717 & -0.0129 & -0.134 \\ 0.0253 & -0.0253 & -0.0504 & 0.0504 \end{bmatrix}$$

i.i.d. Gaussian noise with $\Sigma = \begin{bmatrix} 8.7 & 2.7 \\ 2.7 & 3.2 \end{bmatrix}$

➡ $(0.3, 0.47)$-differential privacy

Simulation



Noise is not added

- user 2 can infer that use 1 consumes electricity

Noise is added

- electricity consumptions are masked
- small degeneration of control performance

Trade off Privacy and Control performances

Summary of Centralized Control

Proposed tracking controller

Design parameters: G_1, L, ω

$$u_p(t) = G_1 x_c(t) + G_2 x_r(t) + \omega(t)$$

$$x_c(t+1) = \left(A_p + \left(B_p + LD_p\right)G_1 + LC_p\right)x_c(t) + \left(B_p + LD_p\right)G_2 x_r(t) - Ly_p(t)$$

Requirements → **Strong stabilization by LMIs**

Stabilization: $A_p + B_p G_1$ and $A_p + LC_p$ are Schur stable

Tracking: $G_2 = U - G_1 X$

Privacy: H_∞-norm of the controller from y_p to u_p is smaller than γ

γ is designed based on $\sigma \geq \gamma c \mathrm{R}(\varepsilon, \delta)$, $\omega \sim \mathcal{N}(0, \sigma)$

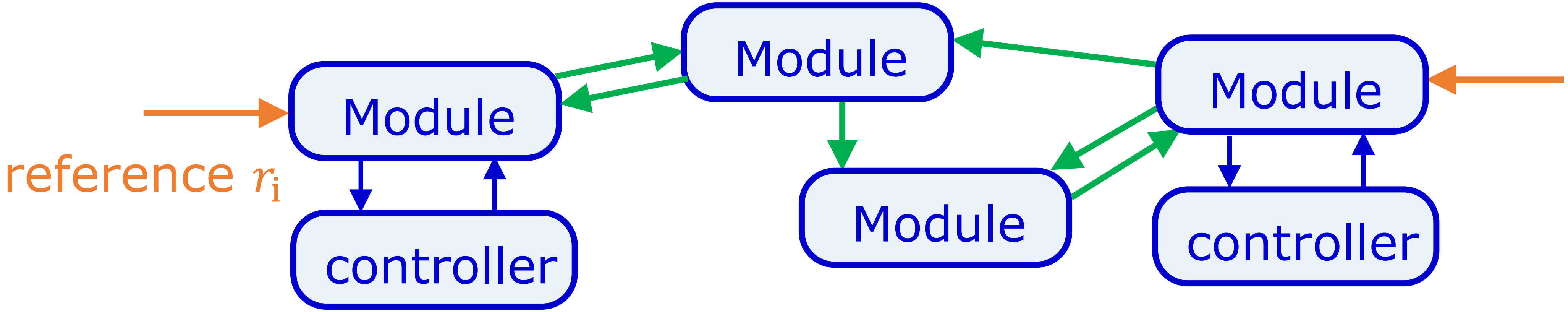
Trade off Privacy and Control performances

Outline

- Differential privacy and input observability

- Control design while addressing privacy concern
  - Centralized tracking control
  - Decentralized tracking control and foundamental trade-off

Problem Formulation Comformed to IoT



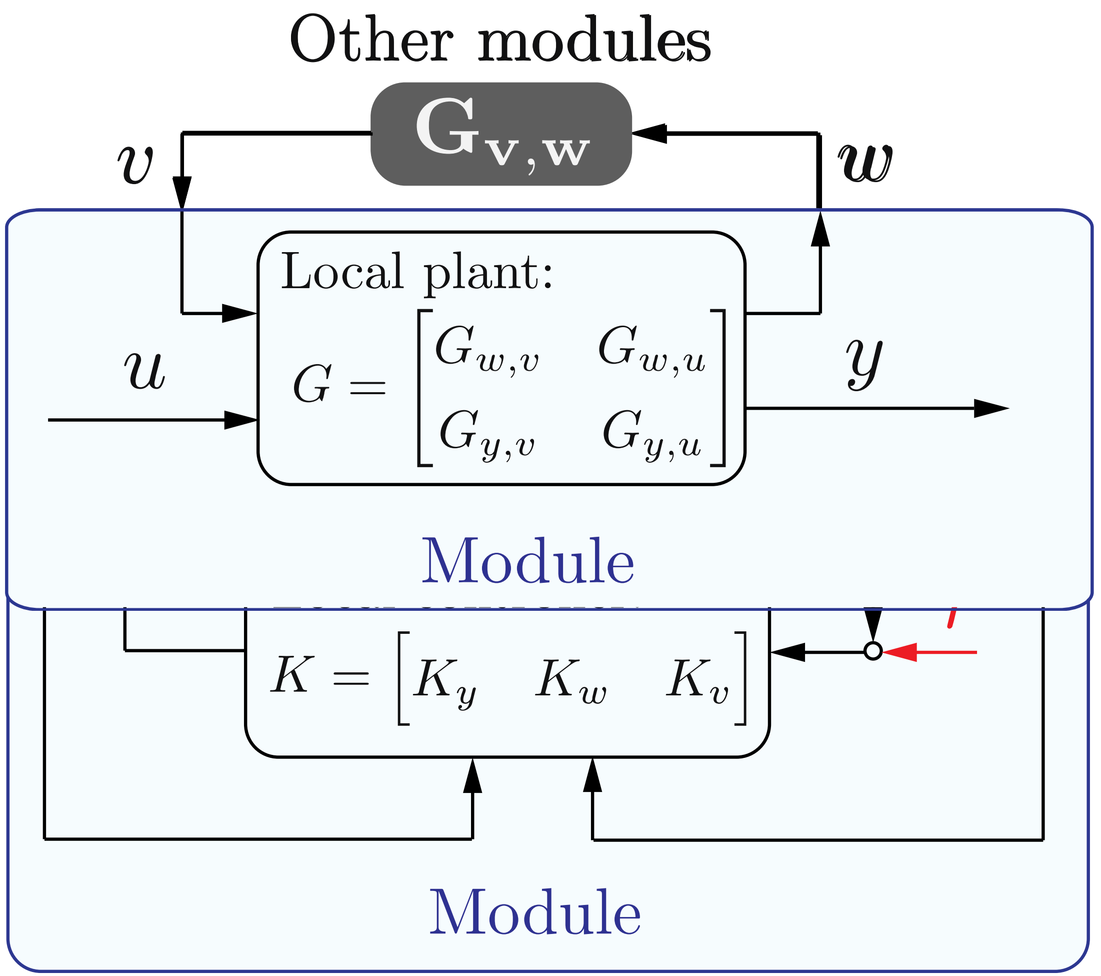
Generally, each module DOES NOT know models of other modules

<u>**Control objective**</u> reference tracking for a module

<u>**Privacy objective**</u> reference needs to be private

How to design a local controller for each module?

Mathematical Formulation for Tracking



Discrete-time linear systems

Objective: $\lim_{t\to\infty}(y - r) = 0$

For local controller design, G, r, y, u, w, v is available but not $\mathbf{G_{v,w}}$

Local controller:

$$u = [K_y \quad K_w \quad K_v] \begin{bmatrix} y - r \\ w \\ v \end{bmatrix}$$

Assumptions

- G and interconnection of G and $\mathbf{G_{v,w}}$ are internally stable
- r is constant

Stability Conditions for Local Controllers

From Youla parametrization, the stabilizing controllers of the module

$$[K_y \quad K_w \quad K_v] = \left(I + Q_y G_{y,u} + Q_w G_{w,u}\right)^{-1} [Q_y \quad Q_w \quad Q_v]$$

Implimentation of a local controller can destroy internal stability of the interconnected system

➡ Retrofit control [Ishizaki et al., Automatica: 19]

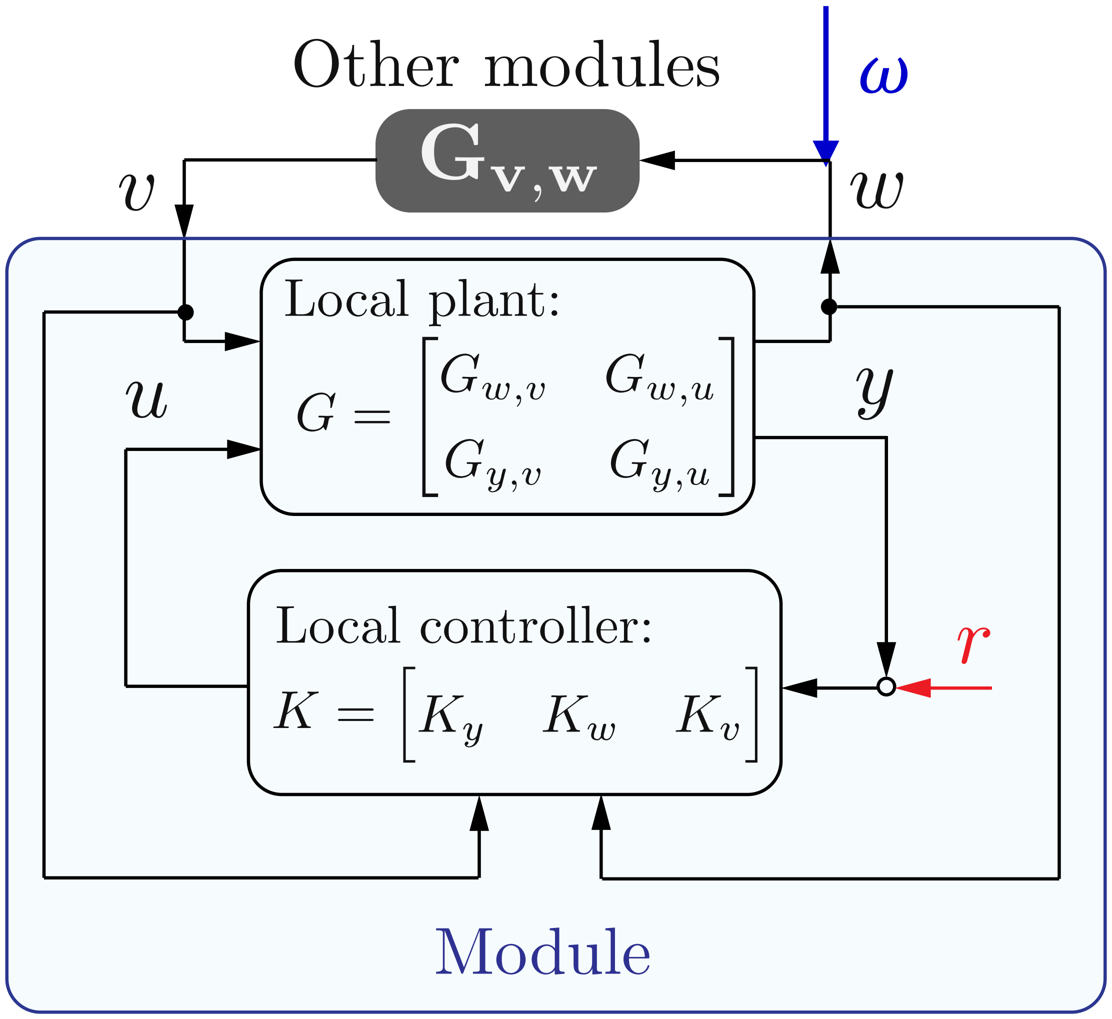
[Thm] Necessary and sufficient conditions for tracking arbitrary constant reference

Stability: $G_{w,u}\left(Q_y G_{y,u} + Q_w G_{w,u} + Q_v\right) = 0$

Tracking: $I + \overline{\mathbf{G}}_{y,r}(1) = 0$

$$\overline{\mathbf{G}}_{y,r} := G_{y,u} + \left(G_{y,v} + G_{y,u}\left(Q_y G_{y,u} + Q_w G_{w,u} + Q_v\right)\right)\left(I - \mathbf{G}_{\mathbf{v},\mathbf{w}} G_{w,v}\right)^{-1} \mathbf{G}_{\mathbf{v},\mathbf{w}} G_{w,u}$$

Privacy Problem of a Module



r can be inferred by other modules from w

We adding noise ω to w to protect from r being infered

How to design ω and K?

<u>$(\boldsymbol{\varepsilon}, \boldsymbol{\delta})$**-differential privacy**</u>

$$\mathbb{P}(y(t) + \omega(t) \in S) \\ \leq e^{\varepsilon}\, \mathbb{P}(y'(t) + \omega(t) \in S) + \delta$$

$(\varepsilon, \delta \geq 0)$

Differential Privacy of Dynamical Systems

Differential privacy is a quantitative criterion for sensitivity of the system with respect to input R_t

$$R_t = \begin{bmatrix} r(0) \\ \vdots \\ r(t) \end{bmatrix} \in \mathbb{R}^{m(t+1)}$$

Induced norm of system (gain) evaluates sensitivity

$$\|\Sigma\|_p := \sup_t \left(\sup_{r_t \neq 0} \frac{|W_t|_p}{|R_t|_p} \right)$$

$$W_t = \begin{bmatrix} w(0) \\ \vdots \\ w(t) \end{bmatrix} \in \mathbb{R}^{p(t+1)}$$

[Thm] For i.i.d. Lapalace noise $\omega \sim \mathrm{Lap}\,(\mu, 2b^2)$, the mechanism is

$(\varepsilon, 0)$-differentially private at any t if and only if

$$b \geq \frac{c}{\varepsilon} \|\Sigma\|_1, \quad \forall |R_t - R_t'|_1 \leq c$$

Peformance Limits for Laplace Mechanism

For the same b, making $\|\Sigma\|_1$ small increases the privacy level

Transfer function from r to w: $-\left(I - G_{w,v}\mathbf{G}_{\mathbf{v,w}}\right)^{-1} G_{w,u} Q_y$

It seems $\|\Sigma\|_1$ can be made arbitrary small by tuning Q_y

However, there are constraints for tuning parameters

$$G_{w,u}\left(Q_y G_{y,u} + Q_w G_{w,u} + Q_v\right) = 0,\ I + \bar{\mathbf{G}}_{\boldsymbol{y,r}}(1) = 0$$

[Thm] If i.i.d. Lapalace mechanism with $\omega \sim \mathrm{Lap}\,(\mu, 2b^2)$ is ε-differentially private at any t, then

$$\varepsilon \geq \frac{c}{b}\left|\left(I - G_{w,v}(1)\mathbf{G}_{\mathbf{v,w}}(1)\right)^{-1} G_{w,u}(1)\, \widehat{\mathbf{G}}_{\mathbf{y,r}}^{-1}(1)\right|_1, \quad \forall |R_t - R_t'|_1 \leq c$$

Example: DC Microgrids

Node i

$$L_i \dot{I}_i = -R_i I_i - V_i + u_i$$
$$C_i \dot{V}_i = I_i - I_{L,i} - \sum_{j \in N_i} R_{i,j}(V_i - \underline{V_j})$$
$$y_i = I_i$$

other modules

I_i : generator current
V_i : load voltage
$I_{L.i}$: load current (constant)

Local controller

$$u_i = K_y I_i + K_w V_i + \sum_{j \in N_i} K_{v_j} V_j, \ j \in N_i$$

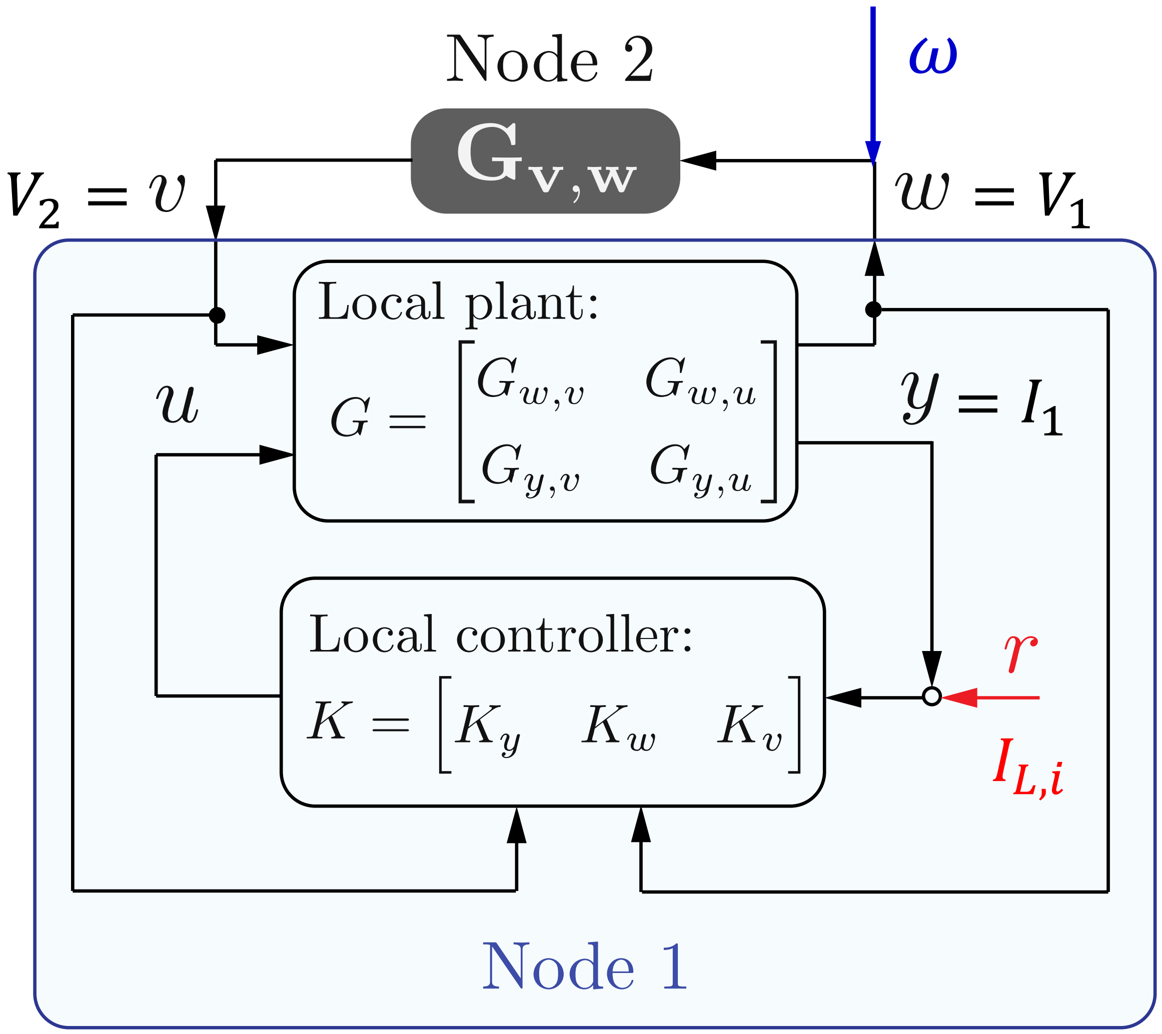
$$[K_y \quad K_w \quad K_v] = \left(I + Q_y G_{y,u} + Q_w G_{w,u}\right)^{-1} [Q_y \quad Q_w \quad Q_v]$$

Control objective

$$\lim_{t \to \infty} I_i(t) = L_{L,i} \qquad \lim_{t \to \infty} V_i(t) = V^*$$

Private info. against others: $I_{L,i}$

Example: DC Microgrids when $n = 2$



Controller design for node 1

Stability: $Q_y G_{y,u} + Q_w G_{w,u} + Q_v = 0$

Tracking: $1 + 1.33 Q_y(1) = 0$

Lower bound on $\|\Sigma\|_1$: 0.25

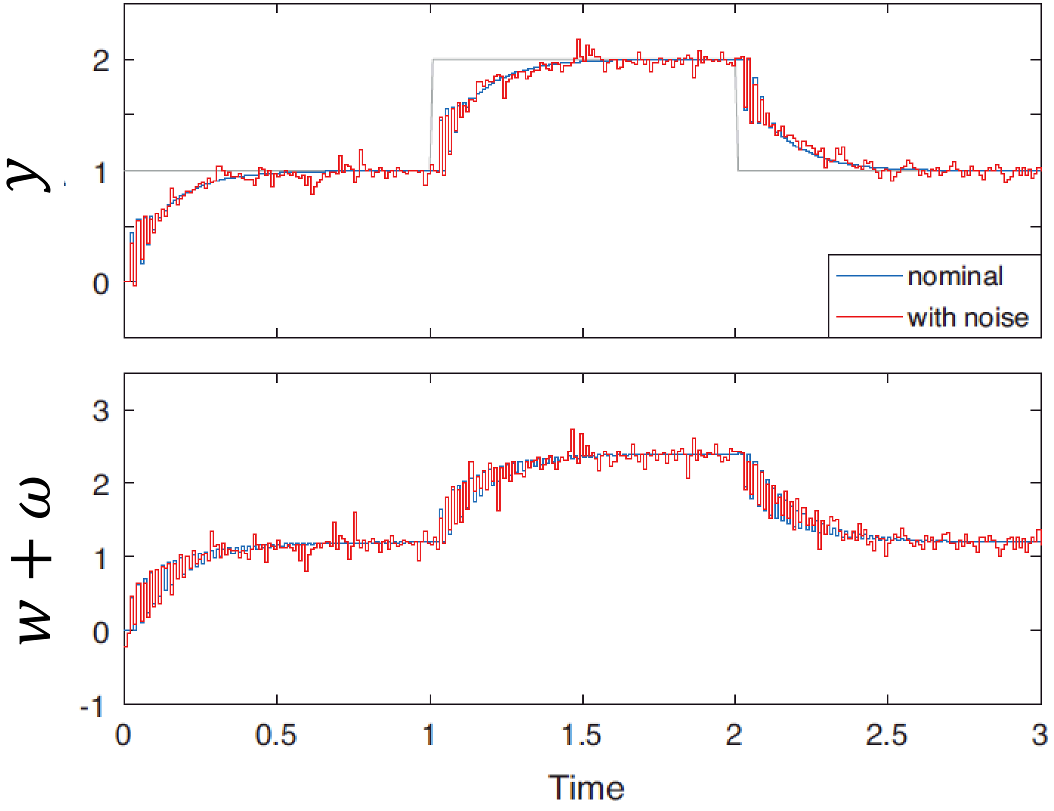
Lower bound on Differential privacy level of Laplace mechanism

$$\varepsilon \geq 0.25c/b$$

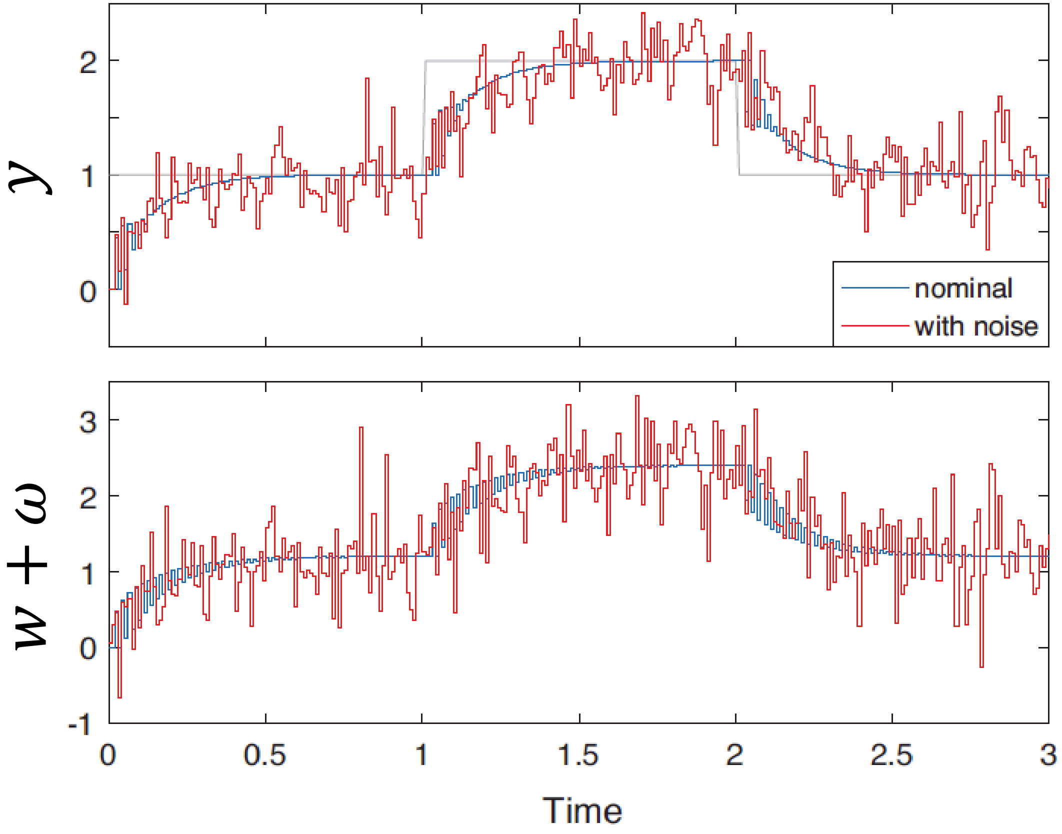
for $\omega \sim \mathrm{Lap}(\mu, 2b^2)$

Simulation

$b = 0.1$



$b = 0.5$



Because of privacy limit, it is impossible to balance tracking and privacy performance by adding noise in modular control design

Summary of Decentrailzed Control

Local tracking controller

$$[K_y \quad K_w \quad K_v] = \left(I + Q_y G_{y,u} + Q_w G_{w,u}\right)^{-1} [Q_y \quad Q_w \quad Q_v]$$

Stability: $G_{w,u}\left(Q_y G_{y,u} + Q_w G_{w,u} + Q_v\right) = 0$

Tracking: $I + \bar{\mathbf{G}}_{\boldsymbol{y},\boldsymbol{r}}(1) = 0$

Design parameters:
Q_y, Q_w, Q_v

Ceiling value of differential privacy level with $\omega \sim \mathrm{Lap}\,(\mu, 2b^2)$

$$\varepsilon \geq \frac{c}{b} \left| \left(I - G_{w,v}(1)\mathbf{G}_{\mathbf{v},\mathbf{w}}(1)\right)^{-1} G_{w,u}(1)\, \widehat{\mathbf{G}}_{\mathbf{y},\mathbf{r}}^{-1}(1) \right|_1, \quad \forall |R_t - R_t'|_1 \leq c$$

Tracking control performance

$$\lim_{t\to\infty} \mathbb{E}[|y(t) - r|_2^2] = 2b^2 \|\Sigma\|_2$$

Trade off

Privacy vs Control

Summary of Talk

Privacy of dynamial system is input observability under noise

- Condition for differential privacy
- Highly input observable ⇔ Less private

Centralized preivacy-preserving tracking control design

- LMI formulation as a strong stabilization problem

Decentralized preivacy-preserving tracking control design

- Ceiling value of differential privacy level

Publications

1. Y. Kawano, M. Cao, “Design of privacy-preserving dynamic controllers,” IEEE TAC 2020
2. Y. Kawano, K. Kashima, M. Cao, “Modular control under privacy protection : Fundamental trade-offs,” Automatica 2021