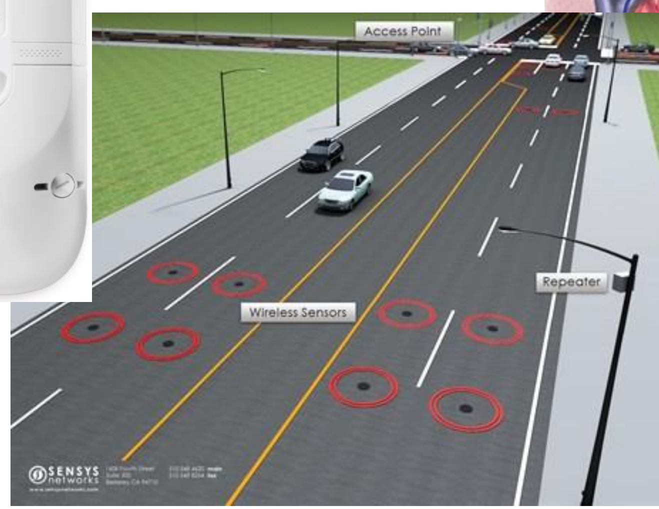
Differential Privacy of Populations in Routing Games

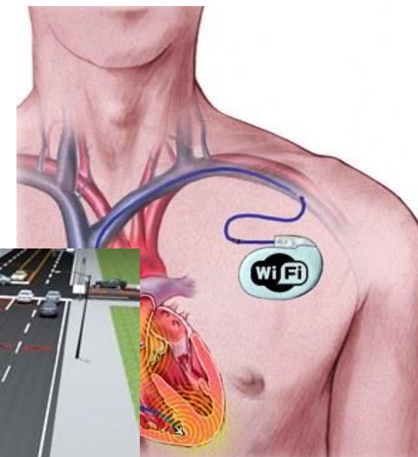
Roy Dong

Joint work with Walid Krichene, Alexandre Bayen, and S. Shankar Sastry

Privacy in Human Cyber-Physical Systems

* **Ubiquity** of sensing and actuation modalities.

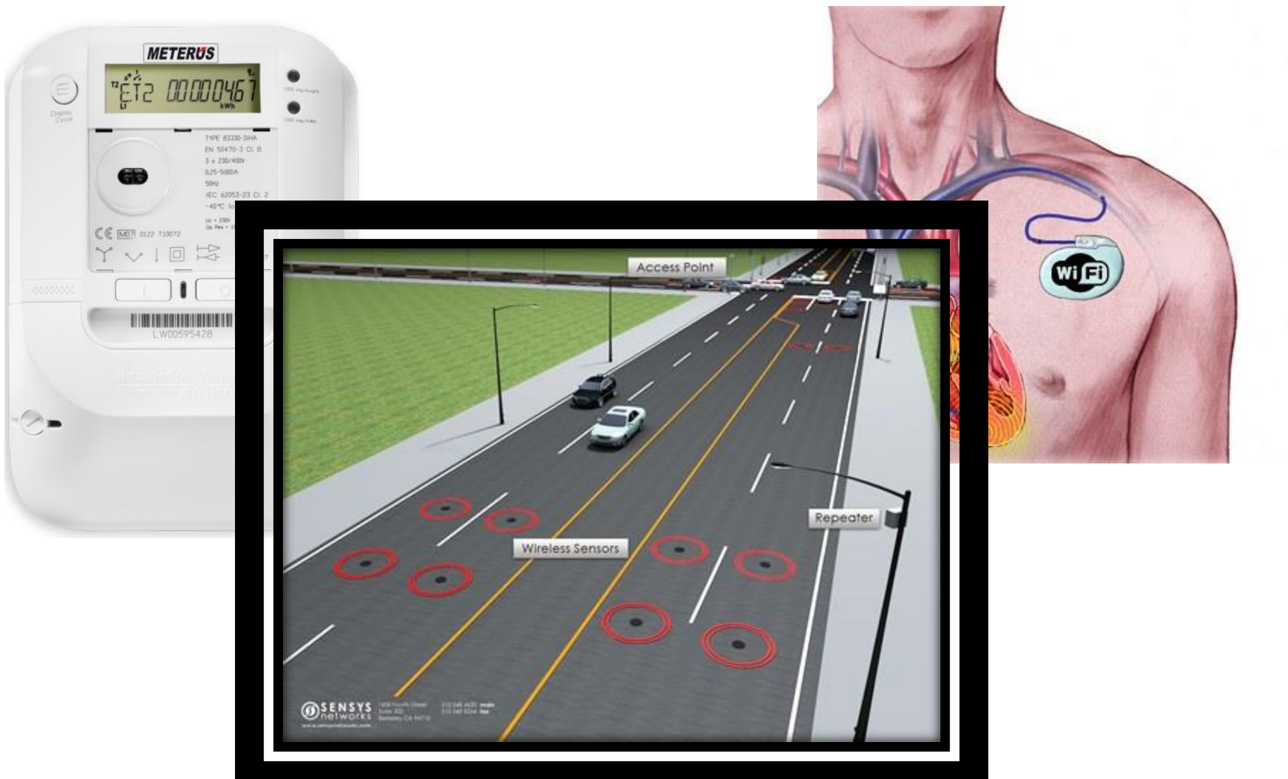




FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Privacy in Human Cyber-Physical Systems

* **Ubiquity** of sensing and actuation modalities.



Privacy

* What conception of privacy are we using?

Privacy

* What type of disclosure are we concerned with?
  * **Identity** disclosure.
  * **Attribute/inferential** disclosure.

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

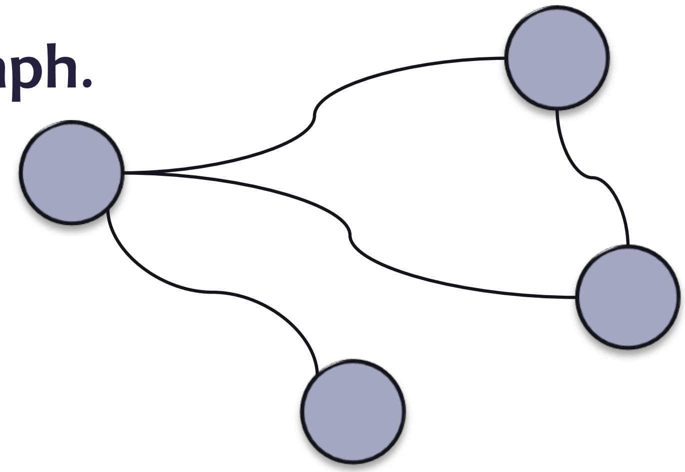
Differential Privacy

* The "gold standard" for database privacy.
  * Pros:
    * Models arbitrary side information.
    * Has "composition" theorems.
  * Cons:
    * Needs an aggregate of a large population.
    * Often needs a noise source of a particular form.

Outline

* Introduction to the Routing Game
* Definitions of Differential Privacy for the Routing Game
* Theoretical Results

The Routing Game



* Represent the traffic network as a **graph**.
* Traffic is abstracted as **flow.**
  * Drivers are **non-atomic.**
* Agents have fixed origins and destinations, and decide which **path** to take.
* The cost of an edge **depends on the total flow** on that edge.

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Definition of the Routing Game

Definition: The *routing game* is given by:

A directed graph $G = (V, E)$.

For each edge $e \in E$, edge cost functions $c_e: \mathbb{R}_+ \to \mathbb{R}_+$.

- These functions are assumed to be non-decreasing and Lipschitz continuous.

A finite set of origin-destination pairs $(o_i, d_i) \in V \times V$, indexed $i \in \{1,2, \dots, I\}$.

A finite set of populations P_k, indexed $k \in \{1,2, \dots, K\}$.

- A population is defined by a vector $\theta_k \in \mathbb{R}_+^I$.

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Actions in the Routing Game

- For each origin-destination pair (o_i, d_i):
  - Let $\mathcal{P}_i$ denote the set of paths that connect o_i to d_i.
  - Then, let:

$$\Delta^{\mathcal{P}_i} = \left\{ m \in \mathbb{R}_+^{|\mathcal{P}_i|} : \sum_{p \in \mathcal{P}_i} m_p = 1 \right\}$$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Actions in the Routing Game

- Populations decide how to allocate mass for each origin-destination pair.
  - For each origin-destination pair (o_i, d_i), the population k chooses how to allocate $(\theta_k)_i$ of flow among the paths connecting o_i to d_i.
  - **Actions:** $x_k \in \Delta^{\mathcal{P}_1} \times \Delta^{\mathcal{P}_2} \times \cdots \times \Delta^{\mathcal{P}_I}$.
- So: $(x_k)_i \in \Delta^{\mathcal{P}_i}$, and population k allocates a flow of $(\theta_k)_i\big((x_k)_i\big)_p$ to $p \in \mathcal{P}_i$.

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Losses in the Routing Game

- Suppose each population picks its action.
- Then, the flow on edge e is:

$$\phi_e(x_1, \dots, x_K) = \sum_{k=1}^{K} \sum_{i=1}^{I} \sum_{\{p \in \mathcal{P}_i : e \in p\}} (\theta_k)_i \big((x_k)_i\big)_p$$

- The loss on path p is:

$$\ell_p(x_1, \dots, x_K) = \sum_{e \in p} c_e\big(\phi_e(x_1, \dots, x_K)\big)$$

- Let $\ell(x_1, \dots, x_K)$ denote the vector of all path losses.

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Losses in the Routing Game

* Finally, the cost for each population k is:

$$\sum_{i=1}^{I} \sum_{p \in \mathcal{P}_i} (\theta_k)_i \big((x_k)_i\big)_p \, \ell_p(x_1, \dots, x_K)$$

* More succinctly:

$$\langle x_k, \ell(x_1, \dots, x_K) \rangle_{\theta_k}$$

FORCES
FOUNDATIONS OF RESILIENT
CYBER-PHYSICAL SYSTEMS

Observation Model

* At each time t, populations observe a noisy version of the loss vector $\hat{\ell}^{(t)}$.

Assumption:

$$\hat{\ell}^{(t)} = \ell\left(x_1^{(t)}, x_2^{(t)}, \ldots, x_K^{(t)}\right) + v_t$$

The v_t are independent across time and identically distributed according to a $N(0, \sigma^2)$ distribution.

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Dynamics of the Routing Game

- How do drivers decide **which path** to take?
  - Based on their new observation and previous decision.

Routing Game Dynamics:

$$x_k^{(t+1)} = \underset{x_k \in \Delta^{\mathcal{P}_1} \times \Delta^{\mathcal{P}_2} \times \cdots \times \Delta^{\mathcal{P}_I}}{\operatorname{argmin}} \langle x_k, \hat{\ell}^{(t)} \rangle_{\theta_k} + \frac{1}{\eta_k^{(t)}} D_{\psi_k}\left(x_k, x_k^{(t)}\right)$$

- Here, D_ψ is the *Bregman divergence* of ψ:

$$D_\psi(x, y) = \psi(x) - \psi(y) - \langle \nabla\psi(y), x - y \rangle$$

FORCES FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Dynamics of the Routing Game

$$x_k^{(t+1)} = \underset{x_k \in \Delta^{\mathcal{P}_1} \times \Delta^{\mathcal{P}_2} \times \cdots \times \Delta^{\mathcal{P}_I}}{\operatorname{argmin}} \langle x_k, \hat{\ell}^{(t)} \rangle_{\theta_k} + \frac{1}{\eta_k^{(t)}} D_{\psi_k}\left(x_k, x_k^{(t)}\right)$$

$\langle x_k, \hat{\ell}^{(t)} \rangle_{\theta_k}$: Minimize losses with respect to the most recent observed loss.

$D_{\psi_k}\left(x_k, x_k^{(t)}\right)$: Penalize large changes.

$\eta_k^{(t)}$: Learning rate for population k.

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

The Routing Game

* In our privacy framework:

  θ : The origins and destinations.

  $u = \psi_e\left(x_1^{(t)}, x_2^{(t)}, \ldots, x_K^{(t)}\right)$: The flow on each edge.

  $y = \hat{\ell}^{(t)}$: The observed congestion.

$$\theta \sim p_\theta$$

$$u \mid \theta \sim p_{u|\theta}$$

$$y \mid u, \theta \sim p_{y|u}$$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Differential Privacy

* Let $Y(\theta) : \theta \mapsto (\hat{\ell}^{(1)}, \hat{\ell}^{(2)}, \ldots, \hat{\ell}^{(T)})$.

Definition:

Two population vectors θ and θ' are *adjacent* if there exists some k such that:

$$||\theta_k - \theta'_k||_\infty \leq c$$

$$\theta_{k'} = \theta'_{k'} \text{ for all } k' \neq k$$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Differential Privacy

Definition:

The routing game is (ϵ, δ) *differentially private* if, for any adjacent θ and θ' if for any measurable set B:

$$P(Y(\theta) \in B) \leq \exp(\epsilon)\, P(Y(\theta') \in B) + \delta$$

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Differential Privacy

Theorem *(Differential privacy of the routing game)*

After T iterations, the mapping $\theta \mapsto \left(\hat{\ell}^{(1)}, \hat{\ell}^{(2)}, \dots, \hat{\ell}^{(T)}\right)$ is (ϵ, δ) differentially private, where:

$$\epsilon = \sum_{t=1}^{T} \epsilon_t \qquad \delta = \sum_{t=1}^{T} \exp\left(\sum_{t'=t+1}^{T} \epsilon_{t'}\right) \delta_t + \delta'$$

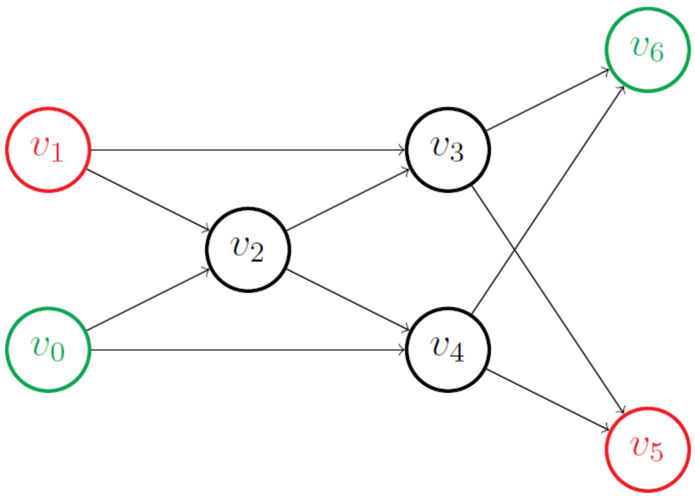
The constants ϵ_t, δ_t, and δ' are such that, for some a:

$$1 - \delta' = \left(1 - 2\exp\left(-\frac{a^2}{2\sigma^2}\right)\right)^{T\,\sum_{i=1}^{I} |\mathcal{P}_i|}$$

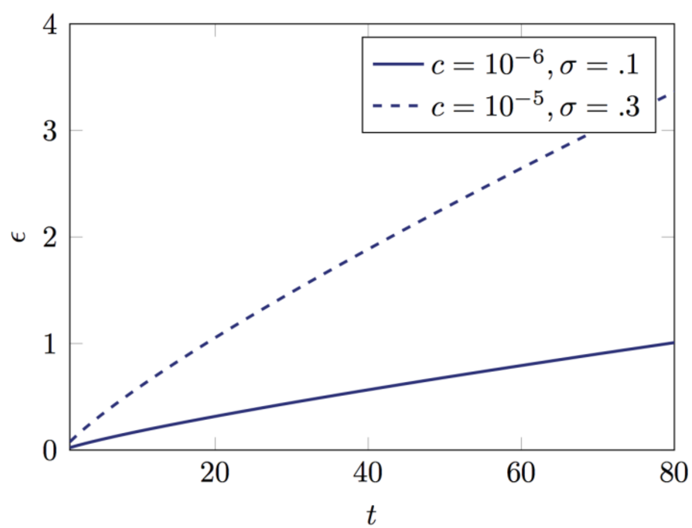
$$\epsilon_t > \frac{c A_\ell A_x \left(2 \ln\left(\frac{1.25}{\delta_t}\right)\right)^{\frac{1}{2}}}{\sigma^2} \times \left[A_\Delta + \frac{A_\theta \max_k \left(\eta_k^{(t)}\right) \left(\sum_{i=1}^{I} |\mathcal{P}_i|\right)^{\frac{1}{2}} (M + a)}{\min_k \ell_{\psi_k}}\right]$$

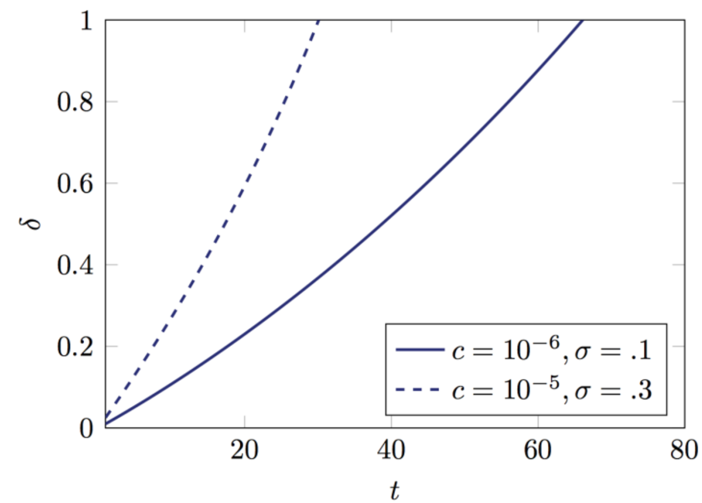
FORCES — FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Routing Game Example



$$\theta \mapsto \left(\hat{\ell}^{(1)}, \hat{\ell}^{(2)}, \ldots, \hat{\ell}^{(T)}\right)$$





Thanks!

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS