Privacy in the Smart Grid: Information, Control & Games*

Vince Poor
Princeton University

Joint work with

V. Belmega, D. Gündüz, S. Kar, S. Mohajer, L. Sankar, et al.

Supported in part by NSF Grants CMMI-14-35778 and ECCS-1549881

* To appear in *Information Theoretic Security and Privacy of Information Systems* (CUP)

Outline

1. Motivation
2. Information: A General Formalism
3. Control: Smart Meter Privacy
4. Games: Competitive Privacy

Motivation

- The smart grid cyber layer generates considerable electronic data:
  - Power flow sensors, phasor measurement units, smart meters, etc.

Motivation

- The smart grid cyber layer generates considerable electronic data:
  - Power flow sensors, phasor measurement units, smart meters, etc.

- This data can leak information that should be kept secure, or private.

Motivation

- The smart grid cyber layer generates considerable electronic data:
  - Power flow sensors, phasor measurement units, smart meters, etc.

- This data can leak information that should be kept secure, or private.
- But, the utility of this data depend on its accessibility.

Motivation

- The smart grid cyber layer generates considerable electronic data:
  - Power flow sensors, phasor measurement units, smart meters, etc.

- This data can leak information that should be kept secure, or private.
- But, the utility of this data depend on its accessibility.
- How can we characterize this fundamental tradeoff?

Information: A General Formalism

[Sankar-Rajagopalan-Poor, T-IFS'13]

Data Source Model

- A sequence of *n* i.i.d. observations of a vector random variable $\mathbf{X} = (X_1\ X_2\ \ldots\ X_K)$ with a joint distribution:

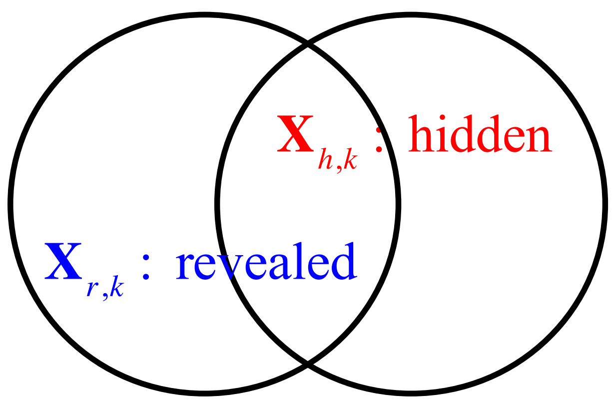
$$\boxed{p_{\mathbf{X}}(\mathbf{x}) = p_{X_1 X_2 \ldots X_K}(x_1, x_2, \ldots, x_K)}$$

Data Source Model

- A sequence of *n* i.i.d. observations of a vector random variable $\mathbf{X} = (X_1\ X_2\ \ldots\ X_K)$ with a joint distribution:

$$\boxed{p_{\mathbf{X}}(\mathbf{x}) = p_{X_1 X_2 \ldots X_K}(x_1, x_2, \ldots, x_K)}$$

- Variables can be divided into public (revealed) and private (hidden) variables, typically not disjoint:



$$k^{th}\ \text{entry} : \mathbf{X}_k = \left(\mathbf{X}_{r,k}, \mathbf{X}_{h,k}\right)$$

Privacy-Utility Tradeoff

- How can we characterize the tradeoff between utility and privacy in such a setting?

Privacy-Utility Tradeoff

- How can we characterize the tradeoff between utility and privacy in such a setting?
  - Measure utility by distortion of the public variables as revealed by the data source; and

Privacy-Utility Tradeoff

- How can we characterize the tradeoff between utility and privacy in such a setting?
  - Measure utility by distortion of the public variables as revealed by the data source; and
  - Measure privacy by equivocation of the private variables in information revealed by the source. (Can also use other leakage measures.)

Privacy-Utility Tradeoff

- How can we characterize the tradeoff between utility and privacy in such a setting?
  - Measure utility by distortion of the public variables as revealed by the data source; and
  - Measure privacy by equivocation of the private variables in information revealed by the source. (Can also use other leakage measures.)
- Then the distortion-equivocation region describes the tradeoff.

Distortion-Equivocation Model

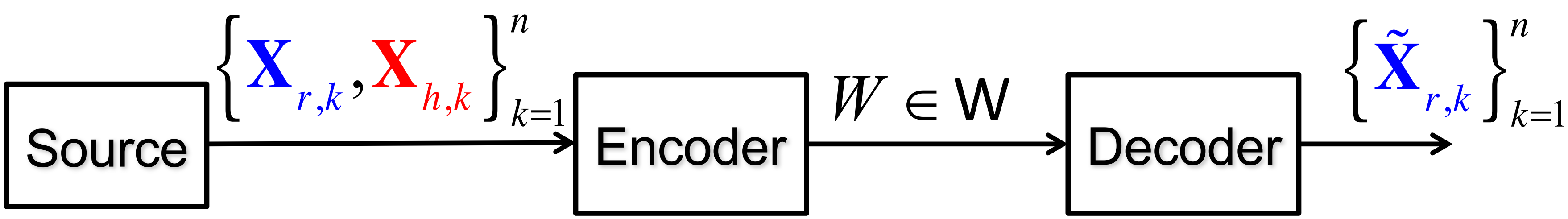
- Encoder maps the original data source to a quantized data source (QDS):

$$\boxed{\text{Encoder}: \mathbf{X}^n \to \mathcal{W} = \left\{QDS_1, QDS_2, \ldots, QDS_M\right\}}$$

Distortion-Equivocation Model

- Encoder maps the original data source to a quantized data source (QDS):

$$\boxed{\text{Encoder}: \mathbf{X}^n \rightarrow \mathcal{W} = \left\{QDS_1, QDS_2, \ldots, QDS_M\right\}}$$



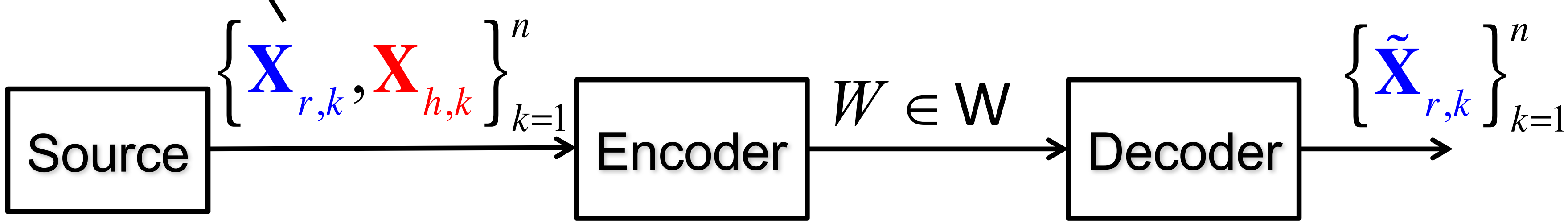
Distortion-Equivocation Model

- Encoder maps the original data source to a quantized data source (QDS):

$$\text{Encoder}: \mathbf{X}^n \rightarrow \mathcal{W} = \left\{ QDS_1, QDS_2, \ldots, QDS_M \right\}$$

Distortion

$$\Delta_d \equiv \mathbb{E}\left[\frac{1}{n} \sum_{i=1}^{n} \rho\left(\mathbf{X}_{r,i}, \tilde{\mathbf{X}}_{r,i} \right) \right] \leq D + \varepsilon$$



Distortion-Equivocation Model

- Encoder maps the original data source to a quantized data source (QDS):

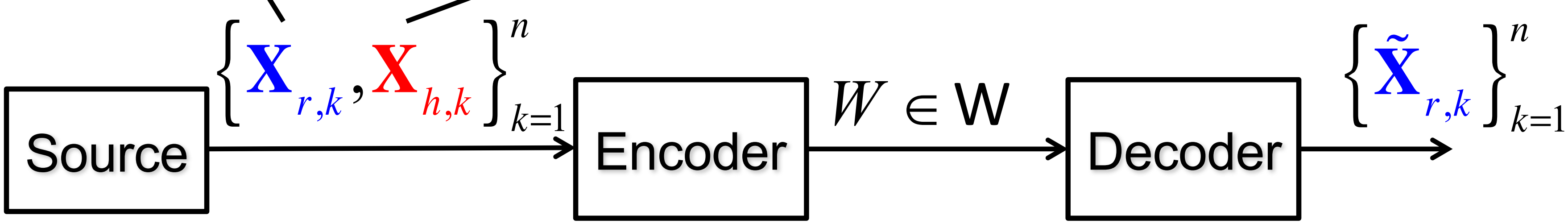
$$\text{Encoder}: \mathbf{X}^n \to \mathcal{W} = \left\{QDS_1, QDS_2, \ldots, QDS_M\right\}$$

Distortion

$$\Delta_d \equiv \mathbb{E}\left[\frac{1}{n}\sum_{i=1}^{n} \rho\left(\mathbf{X}_{r,i}, \tilde{\mathbf{X}}_{r,i}\right)\right] \le D + \varepsilon$$

Equivocation

$$\Delta_p \equiv \frac{1}{n} H\left(\mathbf{X}_h^n \,|\, W\right) > E - \varepsilon$$



Distortion-Equivocation Model

- Encoder maps the original data source to a quantized data source (QDS):

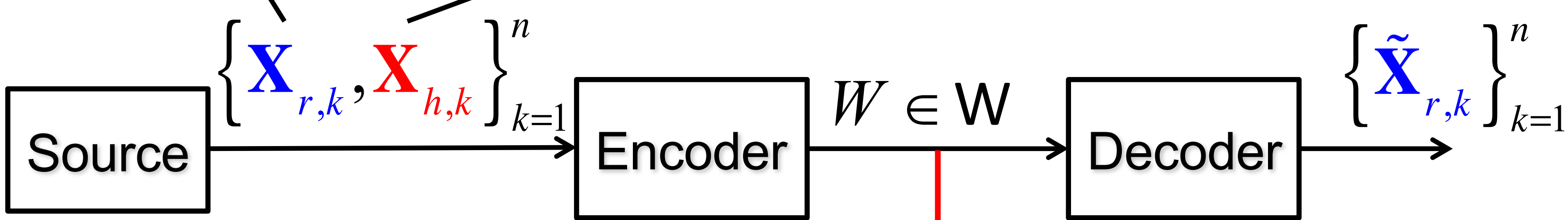
$$\text{Encoder}: \mathbf{X}^n \to \mathcal{W} = \{QDS_1, QDS_2, \ldots, QDS_M\}$$

Distortion

$$\Delta_d \equiv \mathbb{E}\left[\frac{1}{n}\sum_{i=1}^{n} \rho\left(\mathbf{X}_{r,i}, \tilde{\mathbf{X}}_{r,i}\right)\right] \le D + \varepsilon$$

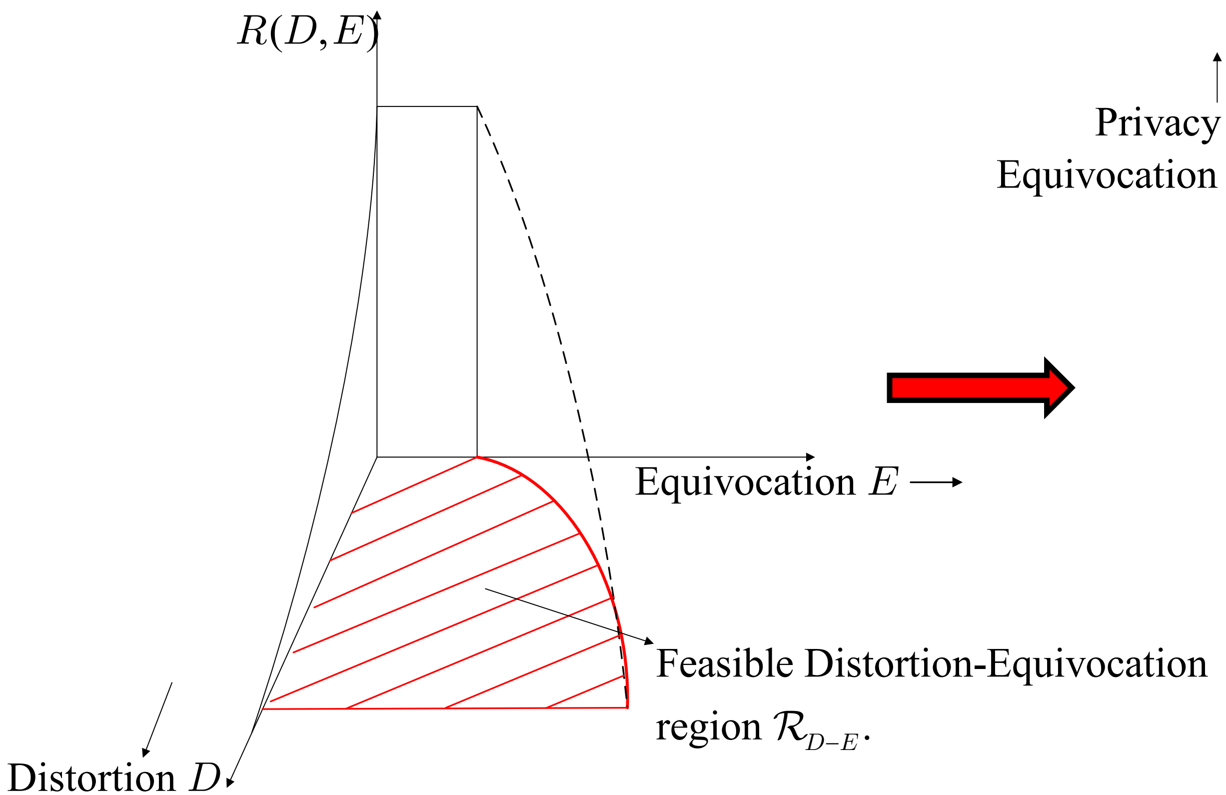
Equivocation

$$\Delta_p \equiv \frac{1}{n} H\left(\mathbf{X}_h^n \mid W\right) > E - \varepsilon$$

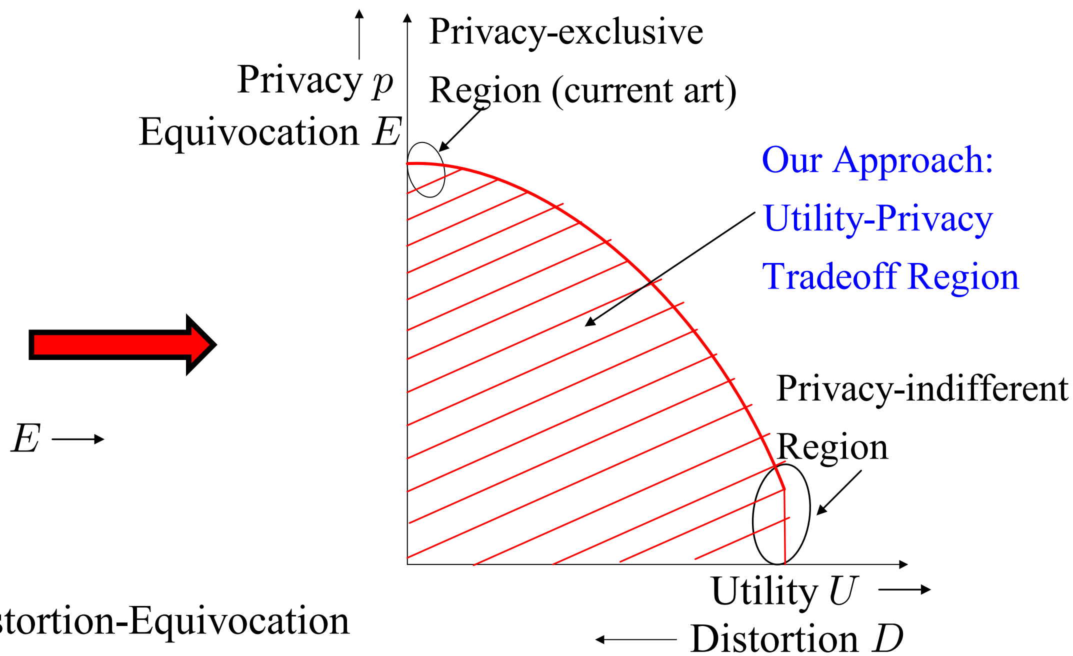


Add a <u>rate constraint</u> → $M \le 2^{n(R+\varepsilon)}$

Utility-Privacy/RDE Regions



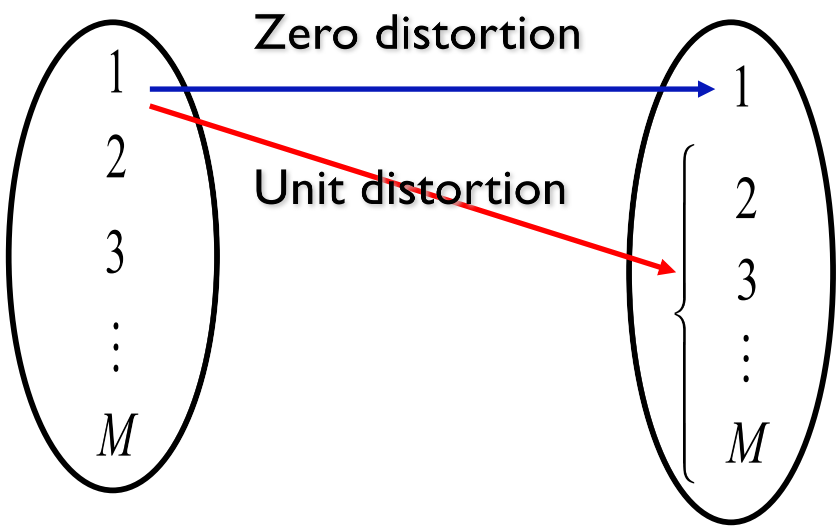
(a): Rate-Distortion-Equivocation Region



(b): Utility-Privacy Tradeoff Region

Example: Categorical Data

- Categorical data: finite alphabet data
  - e.g.: SSN, zipcode, etc.



Original variable X   Distorted variable $\tilde{X}$

Hamming Distortion D :

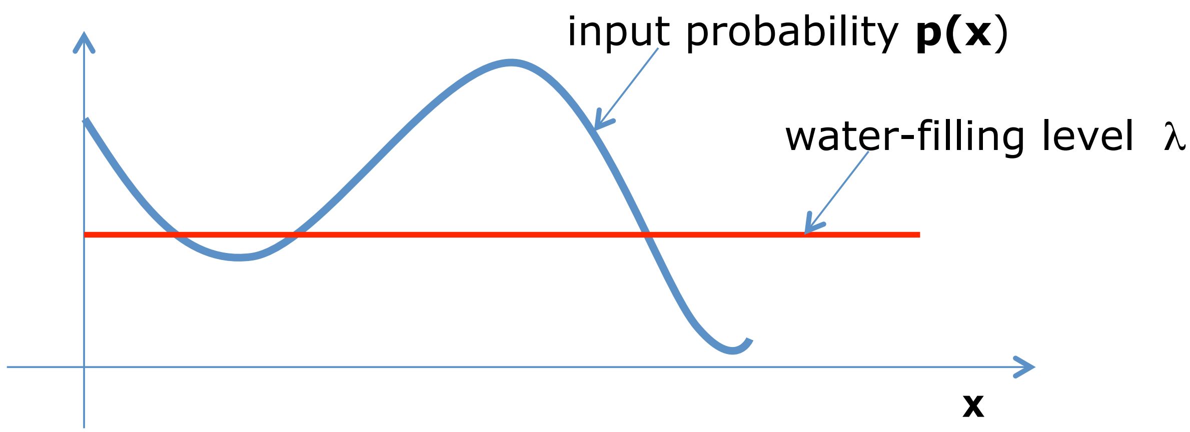
$$D = \Pr(X \neq \tilde{X})$$

Equivocation E :

$$E = H(X \mid \tilde{X})$$

Example: Categorical Data

- Optimal input to output mapping: reverse 'water-filling'
  - Only x with p(x) > λ revealed (λ: water-level).



- Eliminates samples with low probabilities (relative to level λ)
  - Equivalent to outlier aggregation/suppression
  - Such samples reveal the most information
- As D ↑, λ ↑,revealing fewer samples

Summary (General Formalism)

- A data source is divided into private and public variables
  - Leads to an equivocation-distortion characterization
  - Adding rate: a rate-distortion problem with an equivocation constraint

Summary (General Formalism)

- A data source is divided into private and public variables
  - Leads to an equivocation-distortion characterization
  - Adding rate: a rate-distortion problem with an equivocation constraint
- We can also consider
  - multiple sources (side information)
  - other measures of privacy and/or utility

Control:

Smart-Meter Privacy

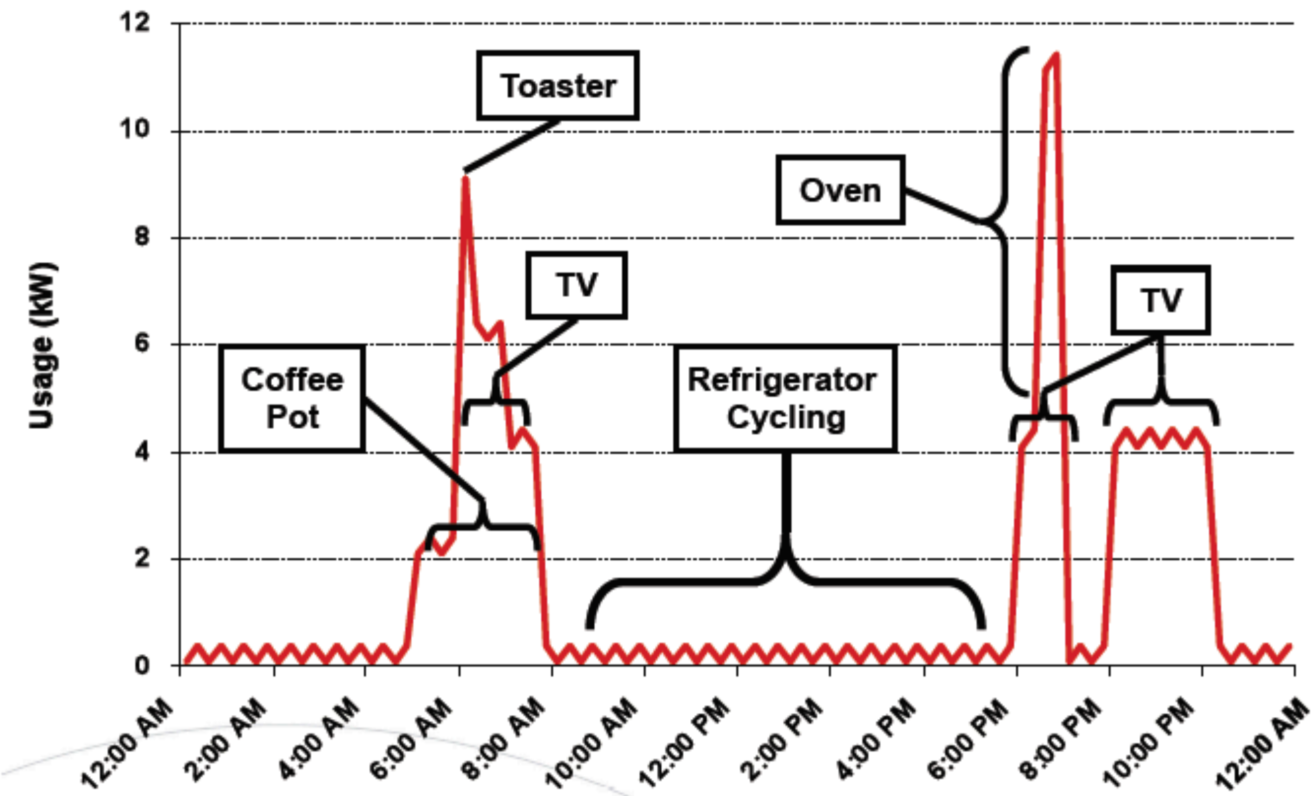
[Sankar-Rajagopolan-Mohajer-Poor, T-SG'13]

[Tan-Gündüz-Poor, JSAC: SG Series'13]

[Yang-Chen-Zhang-Poor, T-SG'15]

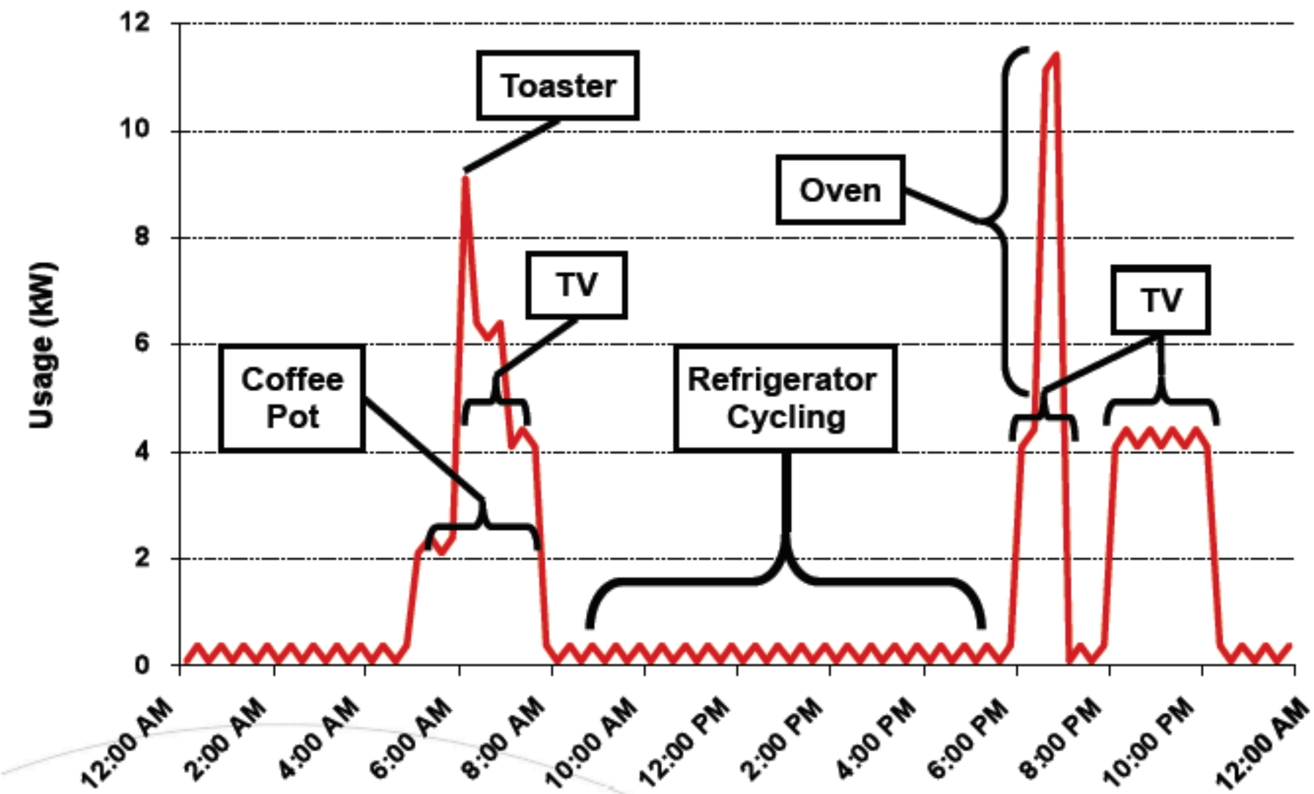
Smart Meter Utility & Privacy

- Smart meter data is useful for price-aware usage, load balancing.



Smart Meter Utility & Privacy

- Smart meter data is useful for price-aware usage, load balancing.
- But, it leaks information about in-home activity.



A Source-Coding Approach

[Sankar-Rajagopolan-Mohajer-Poor, T-SG'13]

<u>Model</u>:

- hidden Gauss-Markov
- hidden state is in {continuous, intermittent}
- encoding of the meter readings

A Source-Coding Approach

[Sankar-Rajagopolan-Mohajer-Poor, T-SG'13]

Model:

- hidden Gauss-Markov
- hidden state is in {continuous, intermittent}
- encoding of the meter readings

Tradeoff:

distortion of usage

versus

information leakage about the intermittent state

A Source-Coding Approach

[Sankar-Rajagopolan-Mohajer-Poor, T-SG'13]

Model:

- hidden Gauss-Markov
- hidden state is in {continuous, intermittent}
- encoding of the meter readings

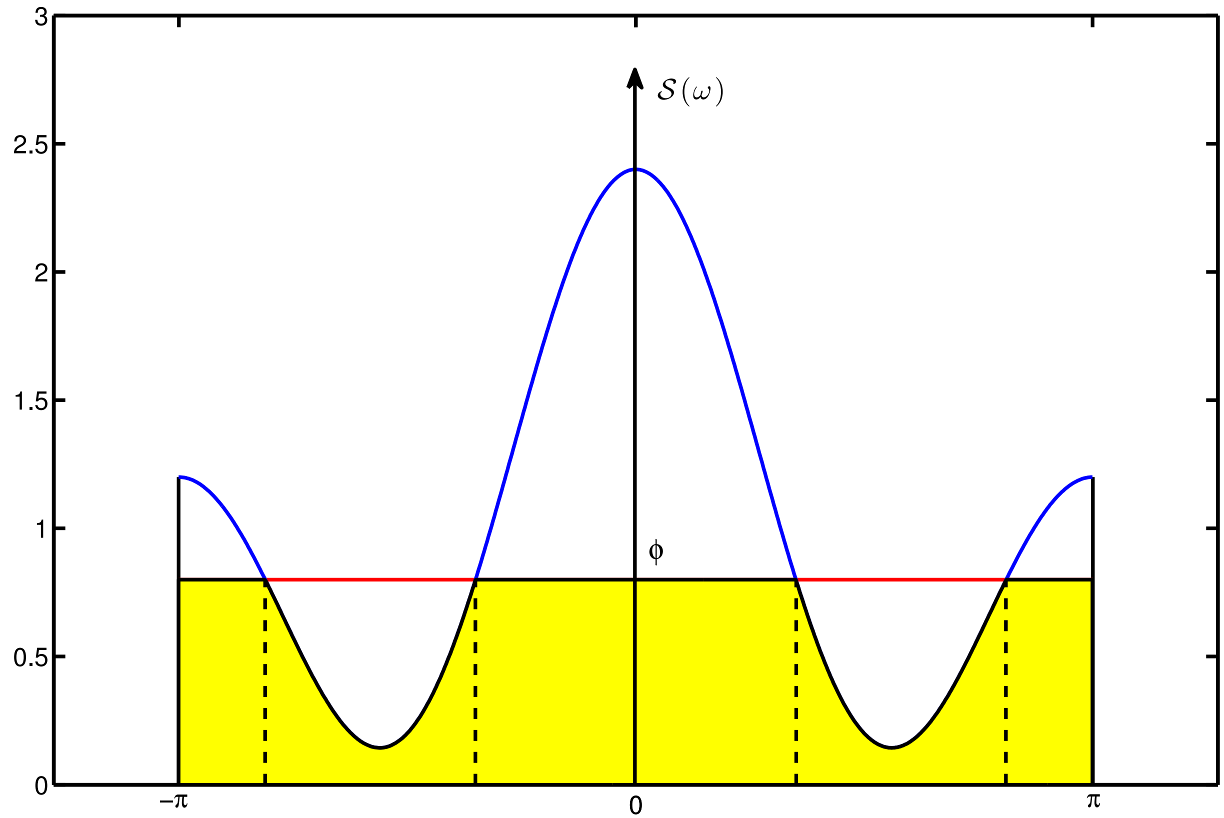
Tradeoff:

distortion of usage
versus
information leakage about the intermittent state

Solution:

a type of "reverse water-filling"
(i.e., rate-minimizing source coding for Gaussian sources)

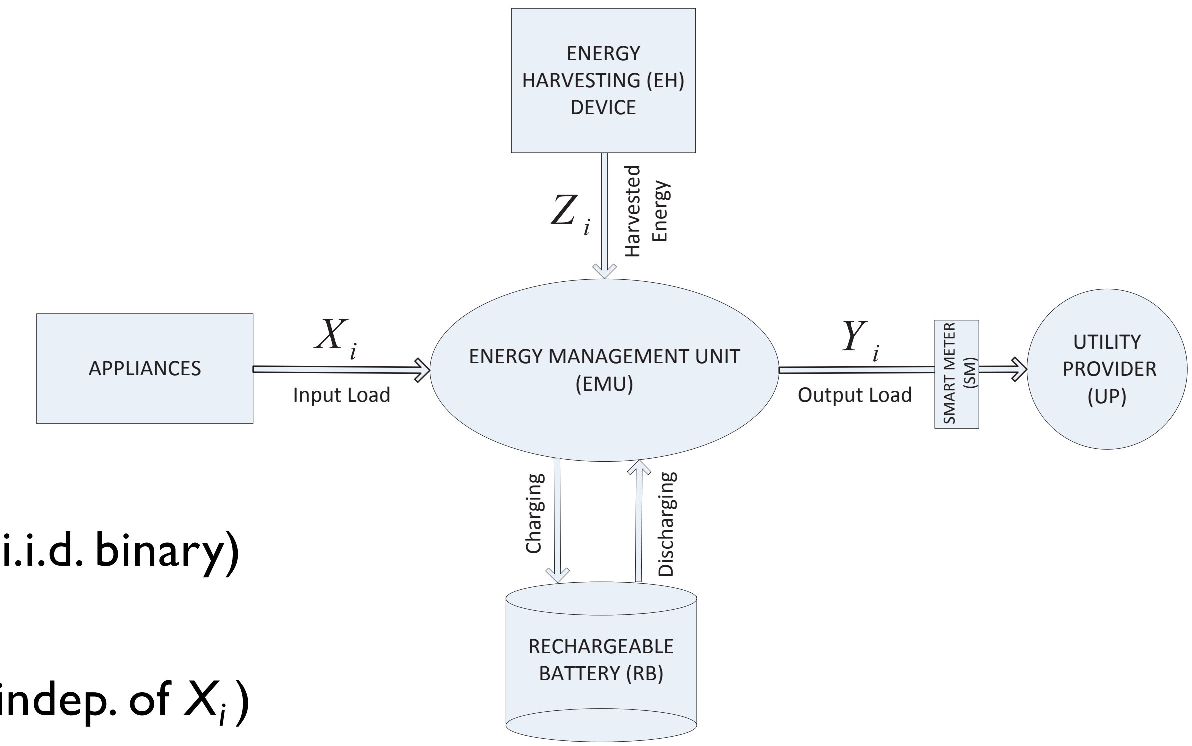
Reverse Water-Filling



A Control Approach

[Tan-Gündüz-Poor, JSAC: SG Series'13]

- Consider situations with energy harvesting (e.g., solar or wind) and rechargeable storage devices (e.g., electric vehicle):



At discrete time i :

- X_i : energy demand of appliances (i.i.d. binary)
- Y_i : energy taken from UP
- Z_i : harvested energy (i.i.d. binary, indep. of X_i)
- B_i : battery state (≤ 1)
- the meter reads and reports Y_i
- (stochastic) control: $(X_i, Z_i, B_{i-1}) \longrightarrow (Y_i, B_i)$ with $X_i \leq Z_i + (B_i - B_{i-1}) + Y_i$

Energy Management Policies

<u>Tradeoff</u>:

wasted energy rate: $P_W^n = \frac{1}{n}\sum_{i=1}^{n}(Z_i + Y_i - X_i)$

versus

information leakage rate: $I^n = \frac{1}{n} I(X^n; Y^n)$

Energy Management Policies

<u>Tradeoff</u>:

wasted energy rate: $P_W^n = \frac{1}{n}\sum_{i=1}^{n}(Z_i + Y_i - X_i)$

versus

information leakage rate: $I^n = \frac{1}{n} I(X^n; Y^n)$

<u>Policy</u>:

transition probabilities: $P(Y_i \mid X_i, Z_i, B_{i-1})$

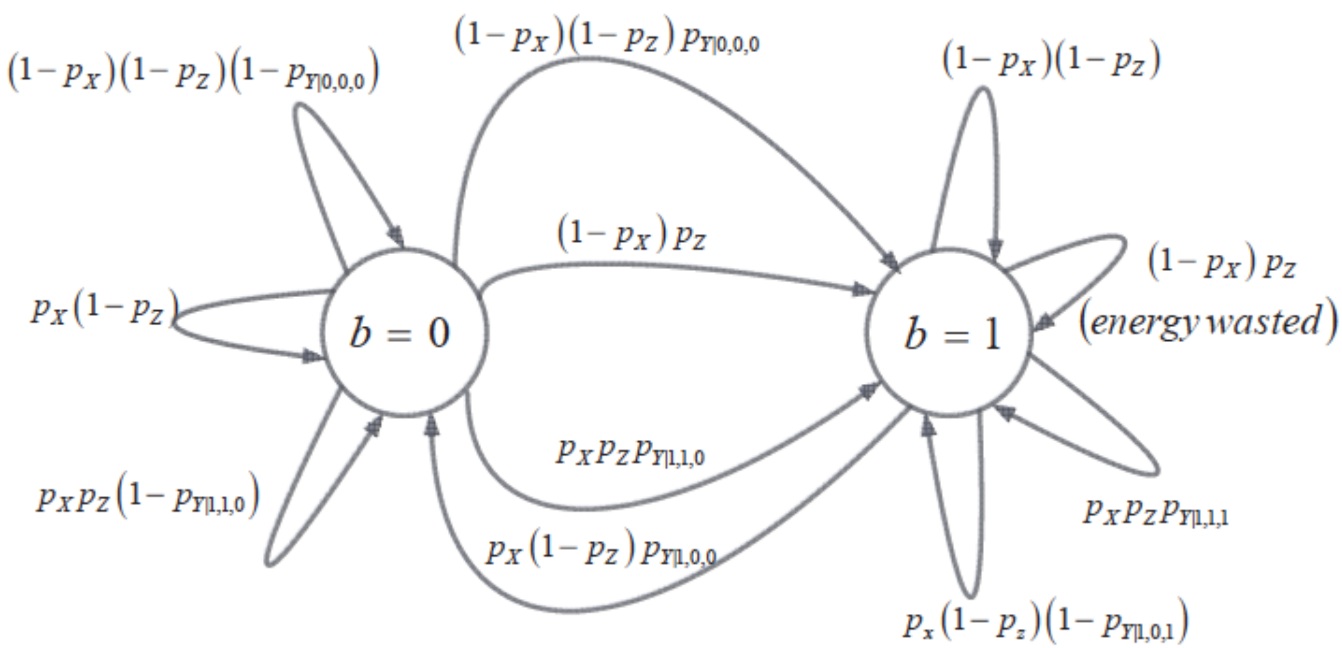
Energy Management Policies

Tradeoff: wasted energy rate: $P_W^n = \frac{1}{n}\sum_{i=1}^{n}(Z_i + Y_i - X_i)$

versus

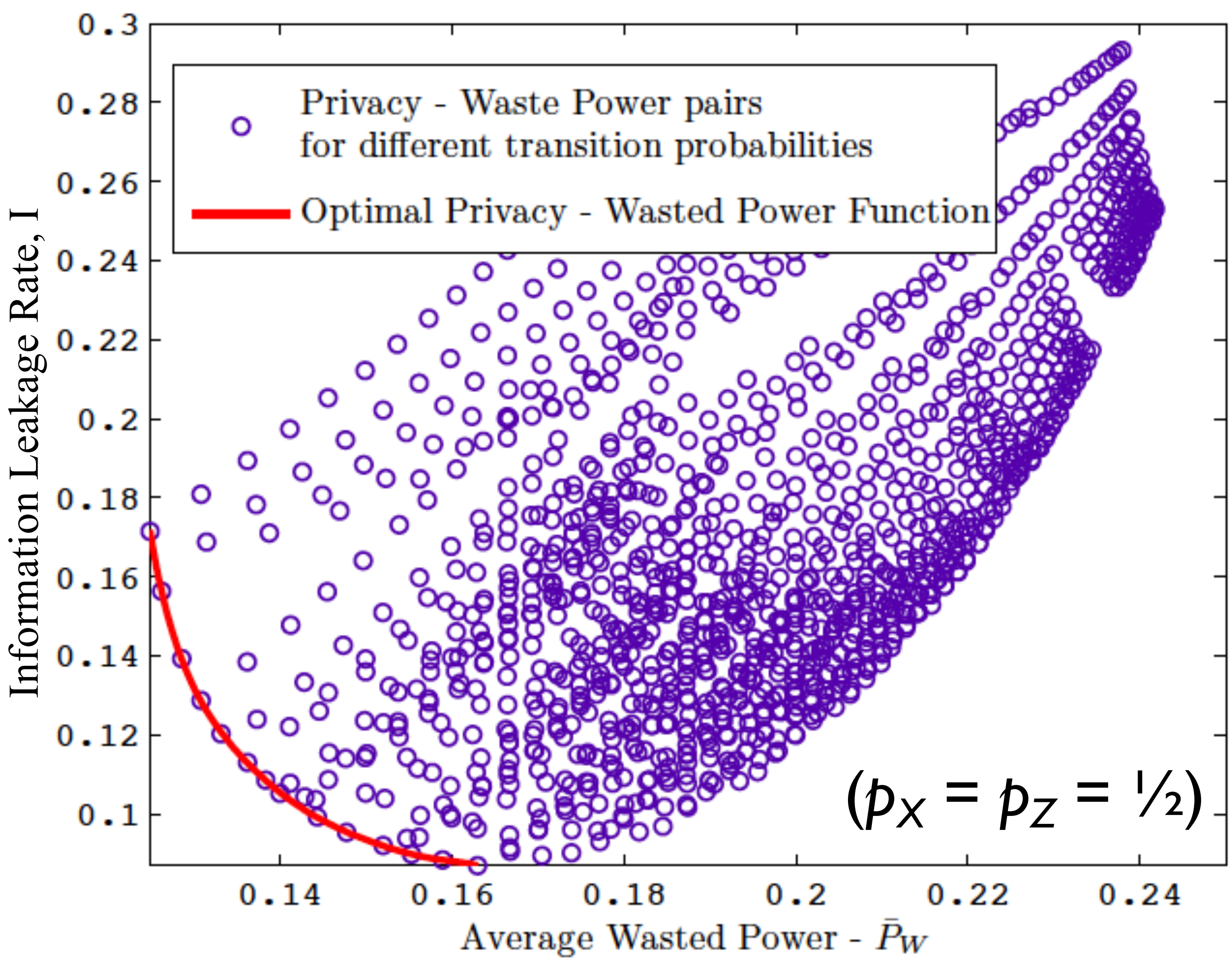
information leakage rate: $I^n = \frac{1}{n} I(X^n;Y^n)$

Policy: transition probabilities: $P(Y_i \mid X_i, Z_i, B_{i-1})$

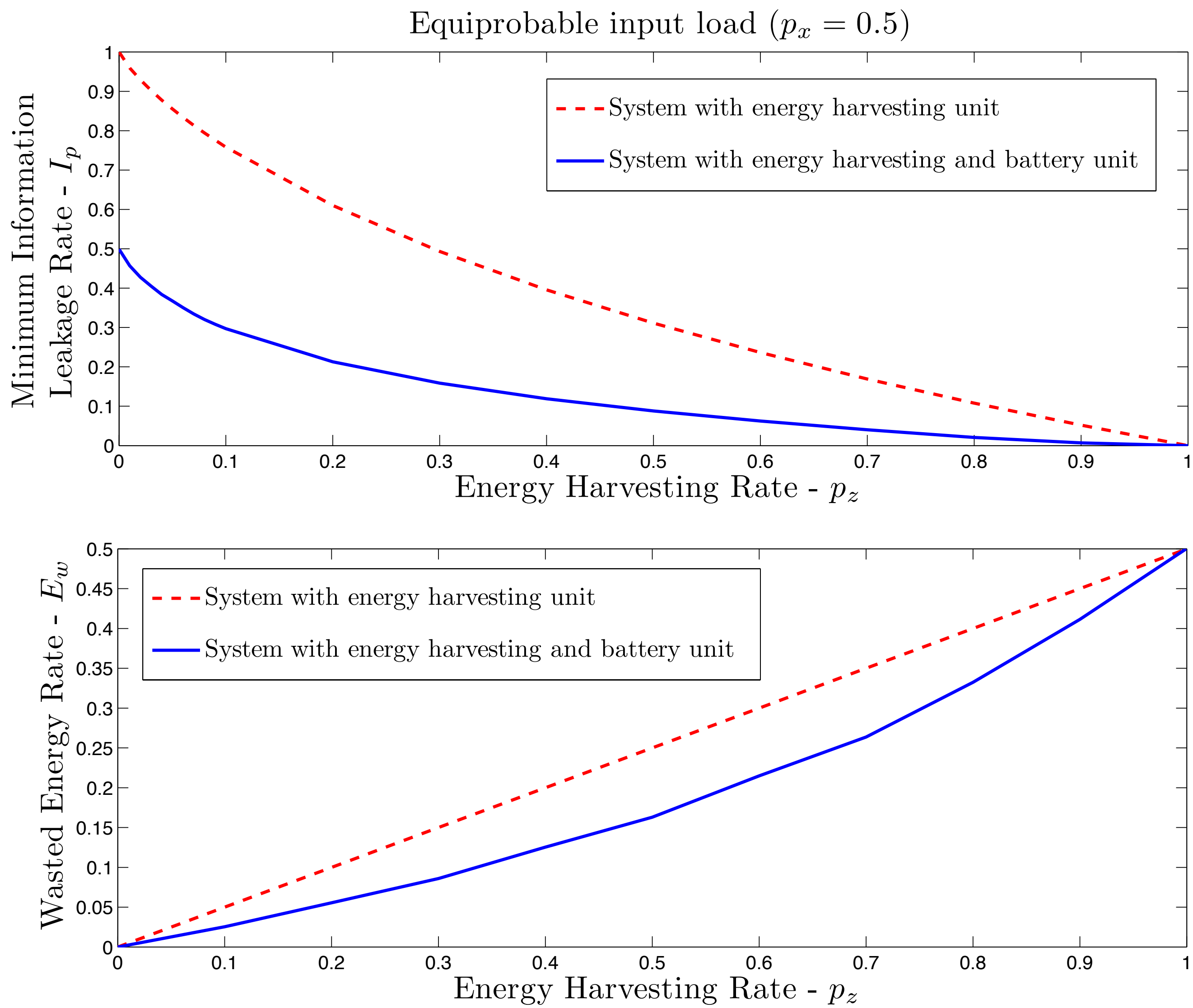


The Privacy-Utility Tradeoff

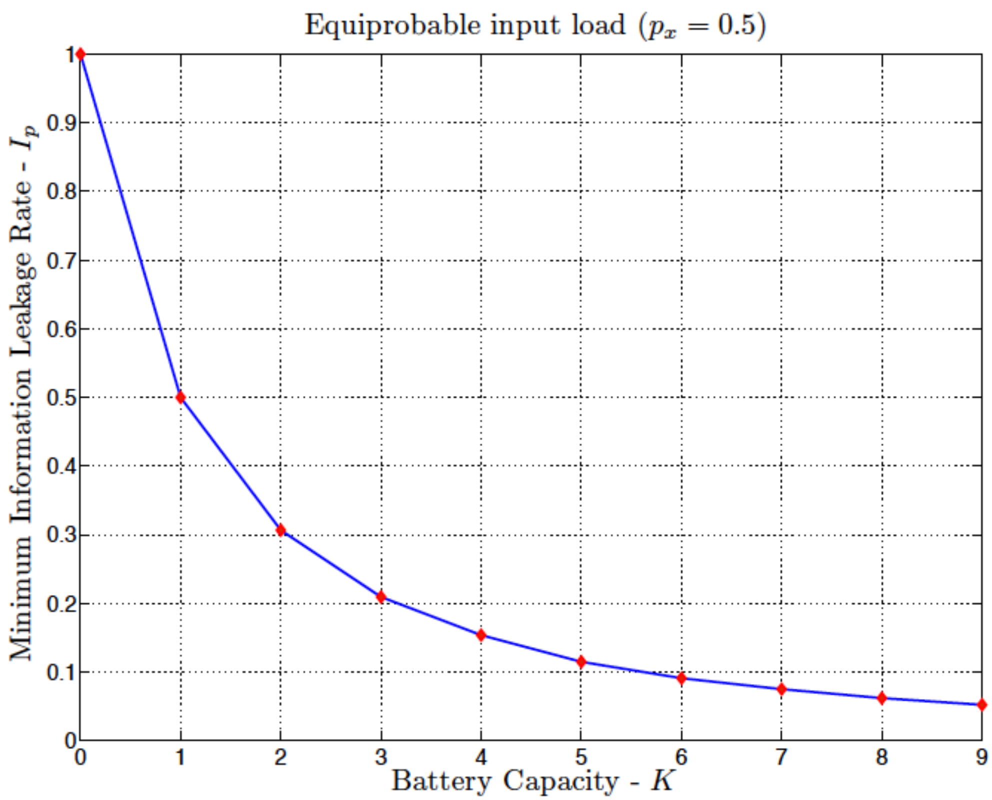
- battery introduces memory: closed form expressions are elusive
- numerically compute mutual information



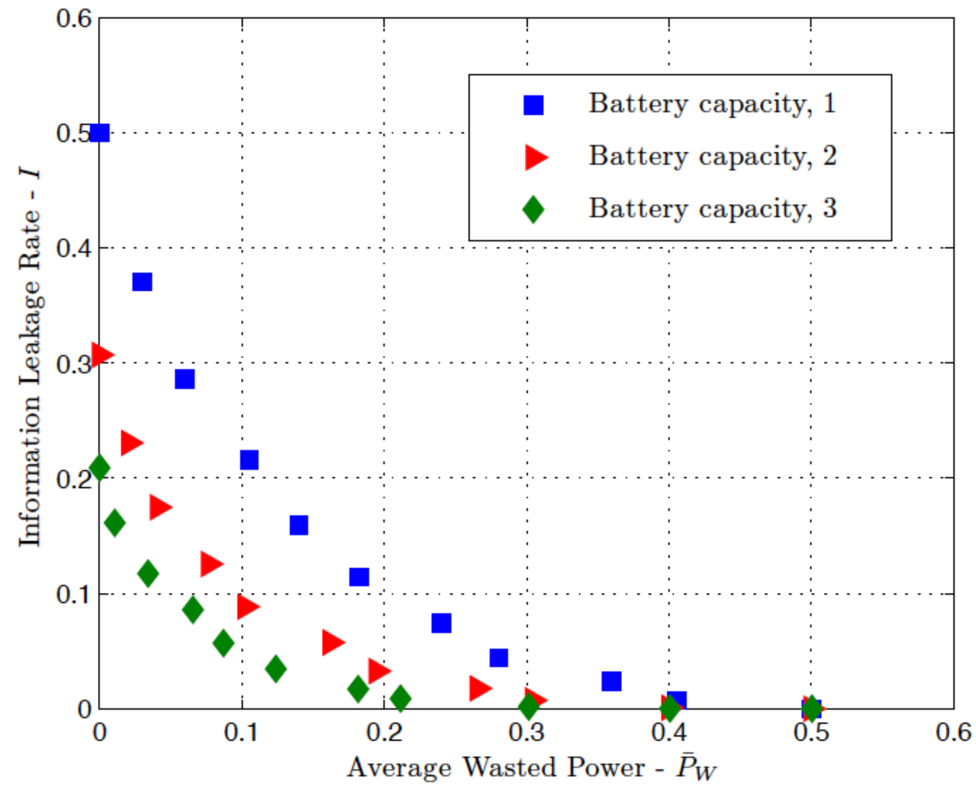
With/ Without a Battery Vs. EH Rate



With No Energy Harvesting



Privacy vs. battery capacity



Tradeoff vs. battery capacity
(allow wasted grid energy)

Summary (Smart Meter Privacy)

- Two approaches to smart meter privacy:
  - source coding at the meter (reverse water filling)
  - control with storage and local supply

Summary (Smart Meter Privacy)

- Two approaches to smart meter privacy:
  - source coding at the meter (reverse water filling)
  - control with storage and local supply
- We can also consider [Yang-Chen-Zhang-Poor, T-SG'15]:
  - adaptive control
  - jointly consider privacy and cost (exploit price variations)

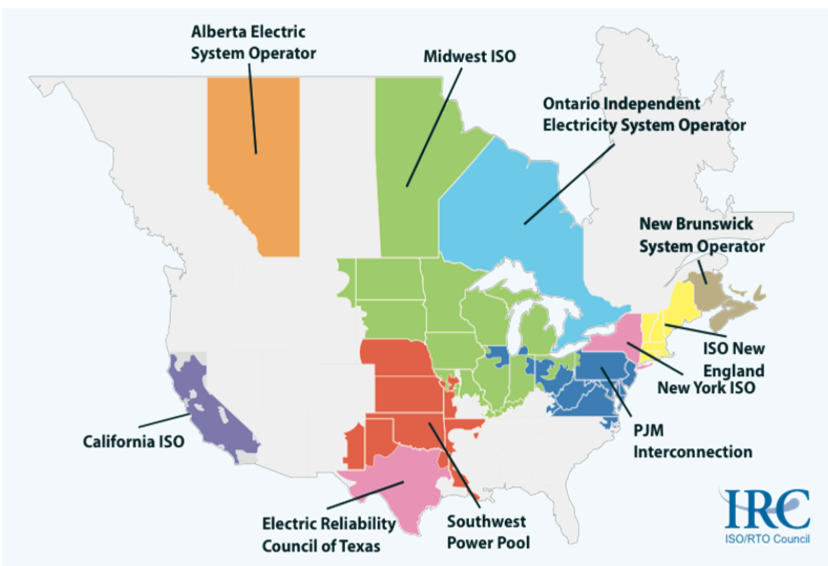
Games:

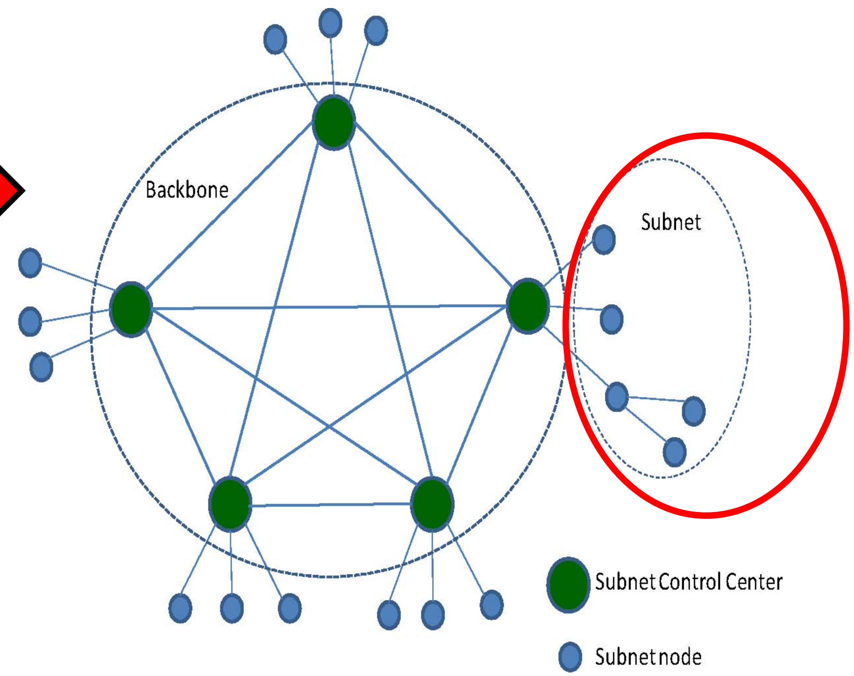
Competitive Privacy

[Belmega-Sankar-Poor, JSTSP'15]

Motivating Example: Multiple RTOs

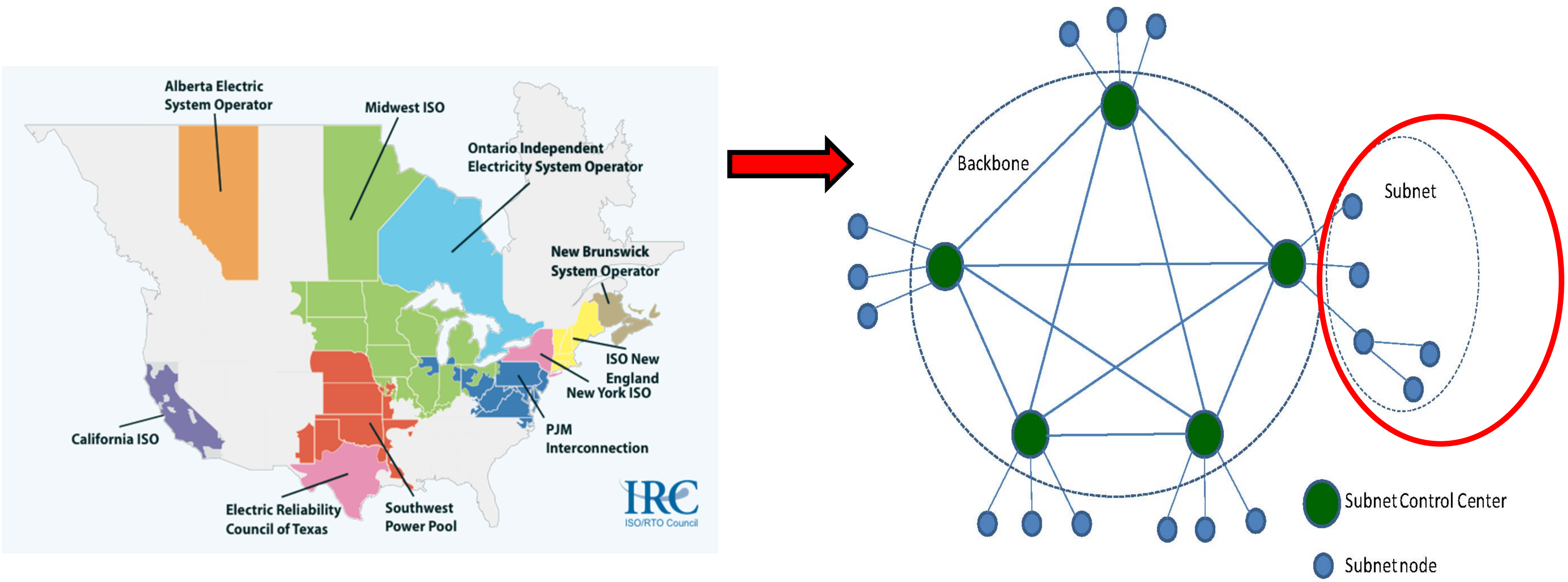
- N.A. Grid: interconnected regional transmission organizations (RTOs)





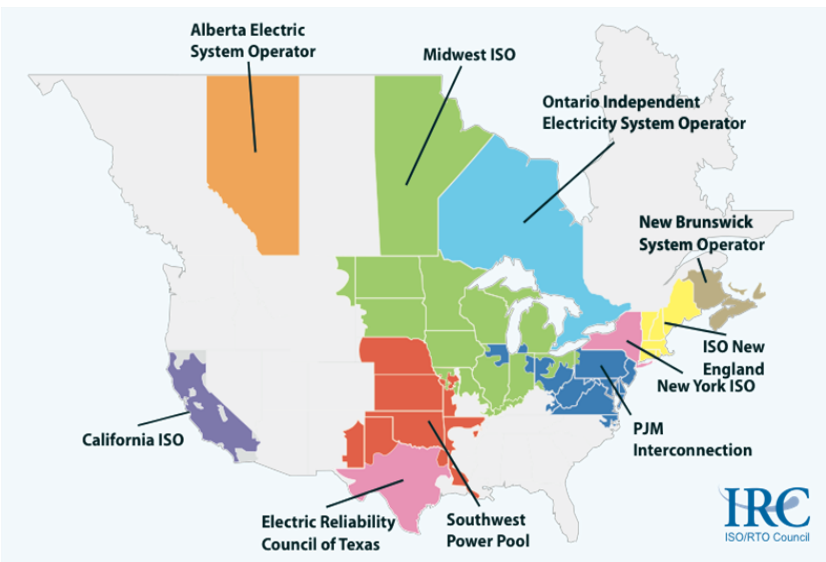
Motivating Example: Multiple RTOs

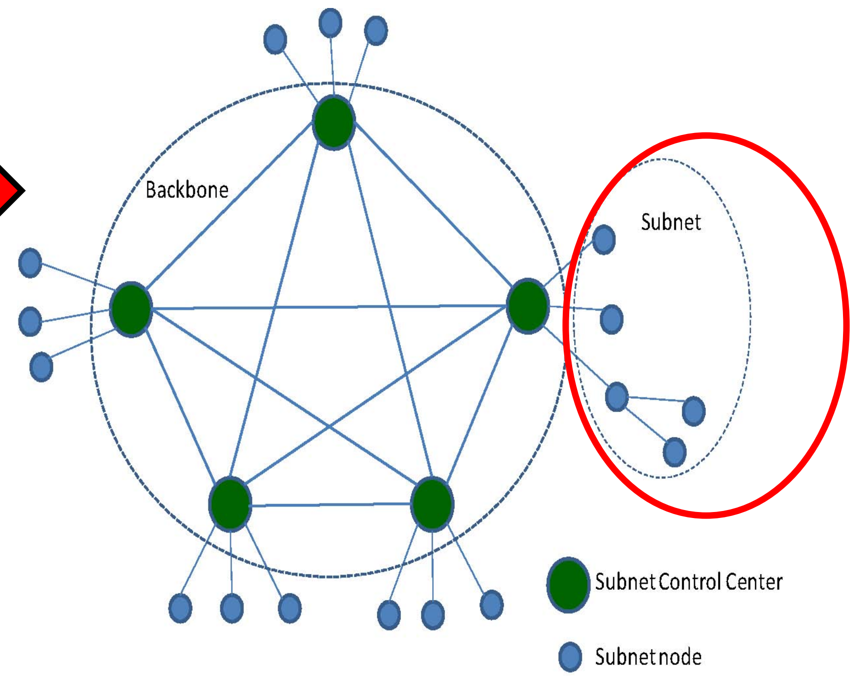
- N.A. Grid: interconnected regional transmission organizations (RTOs) which
  - need to share state measurements for reliability of state estimation (utility)



Motivating Example: Multiple RTOs

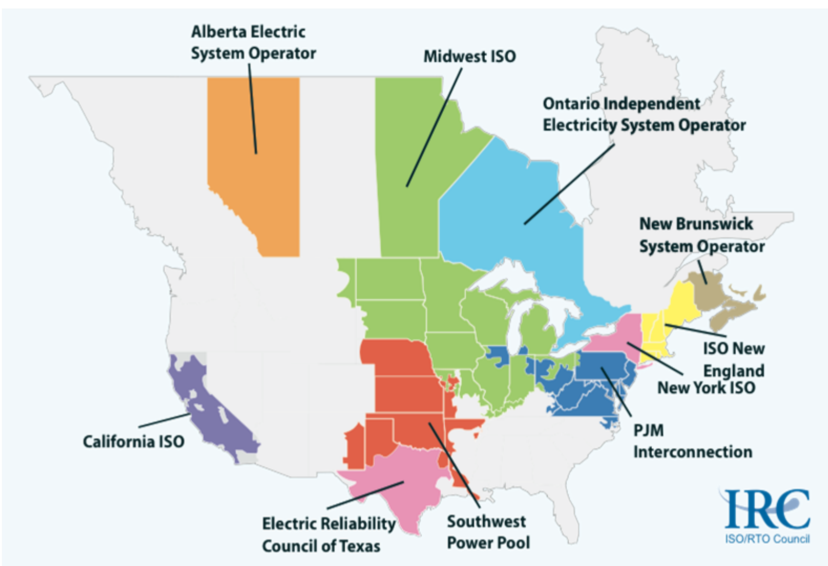
- N.A. Grid: interconnected regional transmission organizations (RTOs) which
  - need to share state measurements for reliability of state estimation (utility)
  - wish to withhold information for economic competitiveness (privacy)

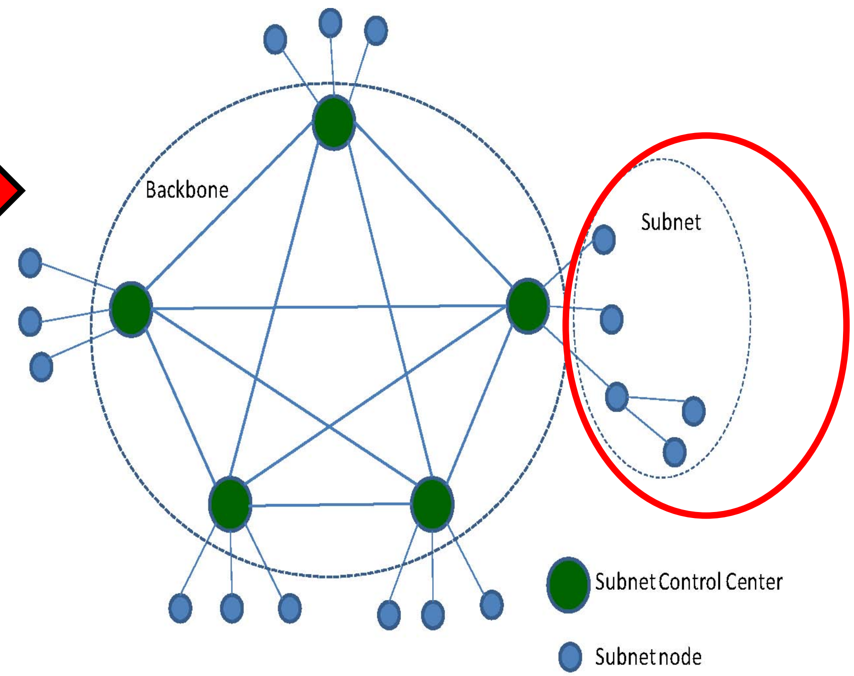




Motivating Example: Multiple RTOs

- N.A. Grid: interconnected regional transmission organizations (RTOs) which
  - need to share state measurements for reliability of state estimation (utility)
  - wish to withhold information for economic competitiveness (privacy)





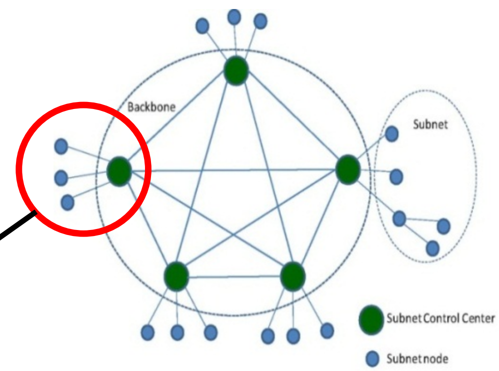
- Leads to a problem of competitive privacy

Competitive Privacy Model

- Noisy measurements at RTO *k*:

$$\boxed{Y_k = \sum_{m=1}^{M} H_{k,m} X_m + Z_k,\ k = 1,2,\ldots,M}$$

m[th] system state

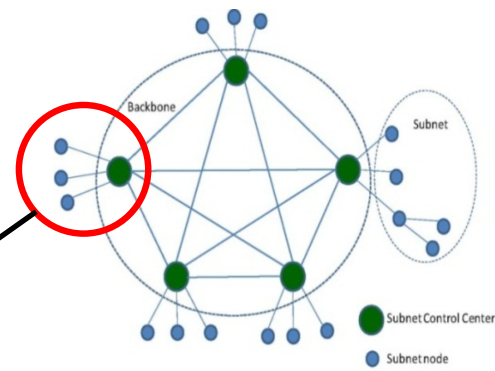


Competitive Privacy Model

- Noisy measurements at RTO *k*:

$$Y_k = \sum_{m=1}^{M} H_{k,m} X_m + Z_k,\ k = 1,2,\ldots,M$$

m^th system state



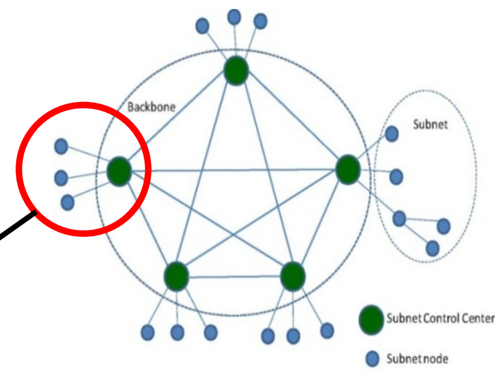
- Cooperation leads to inevitable leakage of state information.

Competitive Privacy Model

- Noisy measurements at RTO *k*:

$$\boxed{Y_k = \sum_{m=1}^{M} H_{k,m} X_m + Z_k,\ k = 1,2,\ldots,M}$$

m^th system state



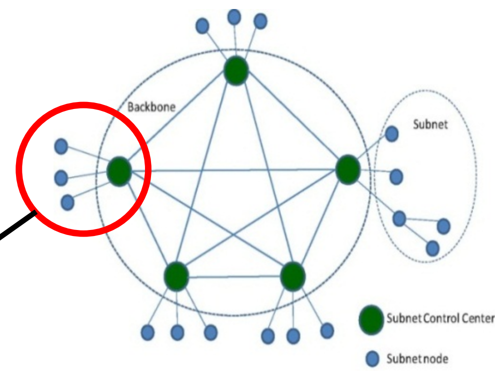
- Cooperation leads to inevitable leakage of state information.
- Utility for RTO *k*: mean-square error for its own state X_k

Competitive Privacy Model

- Noisy measurements at RTO *k*:

$$\boxed{Y_k = \sum_{m=1}^{M} H_{k,m} X_m + Z_k,\ k = 1,2,\ldots,M}$$

m^{th} system state



- Cooperation leads to inevitable leakage of state information.
- Utility for RTO *k*: mean-square error for its own state X_k
- Privacy for RTO *k*: leakage of information about X_k to other RTOs

Two-Agent Case

n i.i.d. observations at each RTO:

$$\boxed{\begin{aligned} Y_{1,i} &= X_{1,i} + \alpha X_{2,i} + Z_{1,i},\ i = 1,\ldots,n \\ Y_{2,i} &= \beta X_{1,i} + X_{2,i} + Z_{2,i},\ i = 1,\ldots,n \end{aligned}}$$

Stochastic model:

$$\boxed{X_{j,i} \sim N(0,1); Z_{2,i} \sim N(0,\sigma_j^2); \text{all indep.}}$$

Two-Agent Case

n i.i.d. observations at each RTO:

$$\boxed{\begin{aligned} Y_{1,i} &= X_{1,i} + \alpha X_{2,i} + Z_{1,i},\ i = 1,\ldots,n \\ Y_{2,i} &= \beta X_{1,i} + X_{2,i} + Z_{2,i},\ i = 1,\ldots,n \end{aligned}}$$

Stochastic model:

$$\boxed{X_{j,i} \sim N(0,1); Z_{2,i} \sim N(0,\sigma_j^2); \text{all indep.}}$$

Tradeoff parameters:

$$\boxed{\begin{aligned} D_j &= \frac{1}{n}\sum_{i=1}^{n} E\left[\left(X_{j,i} - \hat{X}_{j,i}\right)^2\right] \\ L_j &= \frac{1}{n} I\left(X_j^n; J_j, Y_{3-j}^n\right) \end{aligned}}$$

Two-Agent Case

n i.i.d. observations at each RTO:

$$Y_{1,i} = X_{1,i} + \alpha X_{2,i} + Z_{1,i},\ i = 1,\dots,n$$
$$Y_{2,i} = \beta X_{1,i} + X_{2,i} + Z_{2,i},\ i = 1,\dots,n$$

Stochastic model:

$$X_{j,i} \sim N(0,1); Z_{2,i} \sim N(0,\sigma_j^2); \text{all indep.}$$

Tradeoff parameters:

$$D_j = \frac{1}{n}\sum_{i=1}^{n} E\left[\left(X_{j,i} - \hat{X}_{j,i}\right)^2\right]$$
$$L_j = \frac{1}{n} I\left(X_j^n; J_j, Y_{3-j}^n\right)$$

Theorem: Wyner-Ziv coding maximizes privacy (i.e., minimizes L_1 and L_2) for a desired utility at each agent (fixed D_1 and D_2).

Two-Agent Case

n i.i.d. observations at each RTO:

$$Y_{1,i} = X_{1,i} + \alpha X_{2,i} + Z_{1,i},\ i = 1,\ldots,n$$
$$Y_{2,i} = \beta X_{1,i} + X_{2,i} + Z_{2,i},\ i = 1,\ldots,n$$

Stochastic model:

$$X_{j,i} \sim N(0,1); Z_{2,i} \sim N(0,\sigma_j^2); \text{all indep.}$$

Tradeoff parameters:

$$D_j = \frac{1}{n}\sum_{i=1}^{n} E\left[\left(X_{j,i} - \hat{X}_{j,i}\right)^2\right]$$
$$L_j = \frac{1}{n} I\left(X_j^n; J_j, Y_{3-j}^n\right)$$

Theorem: Wyner-Ziv coding maximizes privacy (i.e., minimizes L_1 and L_2) for a desired utility at each agent (fixed D_1 and D_2).

But, L_j depends on D_{3-j} (not D_j), so how should each agent choose to behave?

Two-Agent Case

n i.i.d. observations at each RTO:

$$Y_{1,i} = X_{1,i} + \alpha X_{2,i} + Z_{1,i},\ i = 1,\ldots,n$$
$$Y_{2,i} = \beta X_{1,i} + X_{2,i} + Z_{2,i},\ i = 1,\ldots,n$$

Stochastic model:

$$X_{j,i} \sim N(0,1); Z_{2,i} \sim N(0,\sigma_j^2); \text{all indep.}$$

Tradeoff parameters:

$$D_j = \frac{1}{n}\sum_{i=1}^{n} E\left[\left(X_{j,i} - \hat{X}_{j,i}\right)^2\right]$$
$$L_j = \frac{1}{n} I\left(X_j^n; J_j, Y_{3-j}^n\right)$$

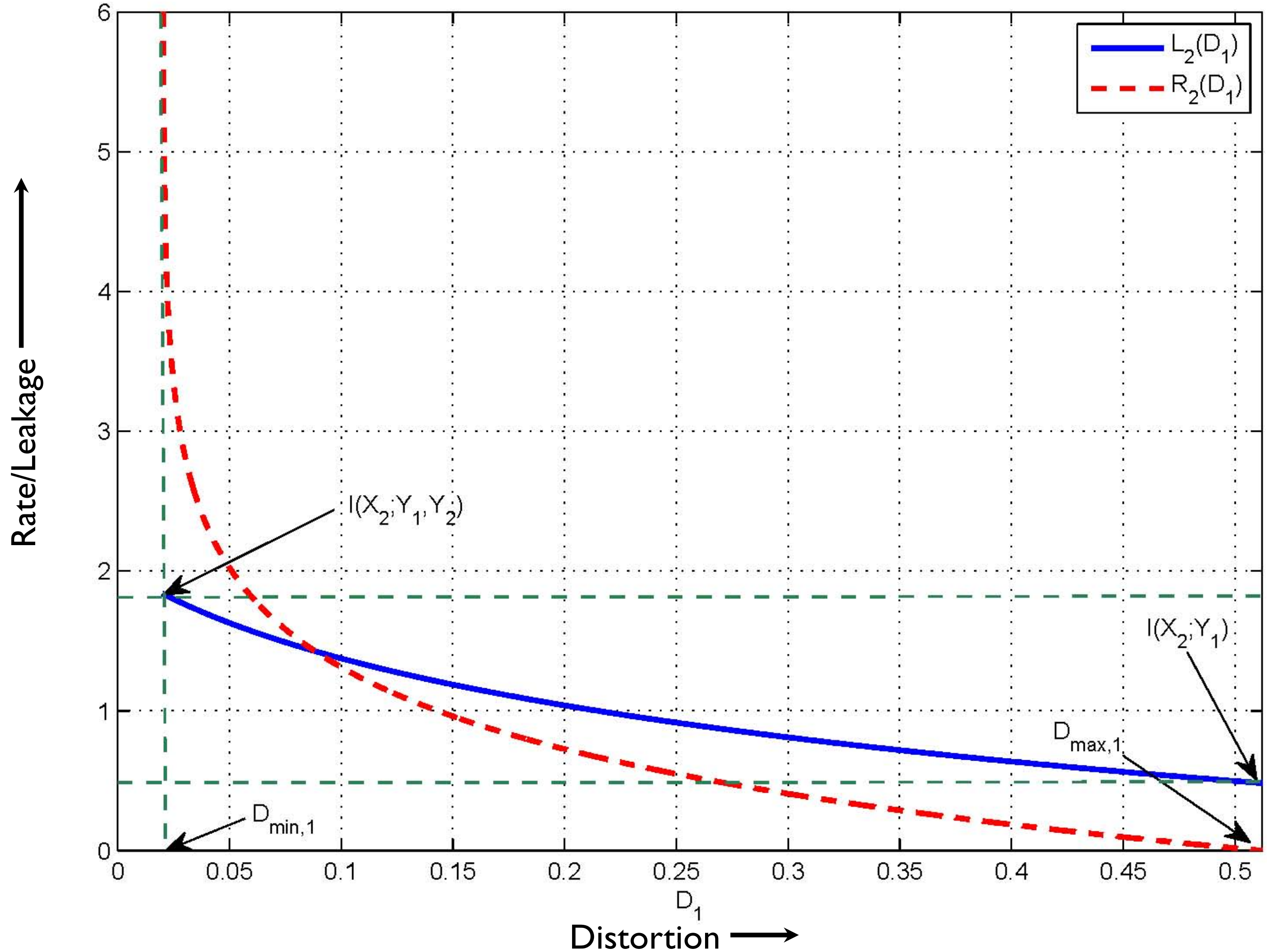
<u>Theorem</u>: Wyner-Ziv coding maximizes privacy (i.e., minimizes L_1 and L_2) for a desired utility at each agent (fixed D_1 and D_2).

But, L_j depends on D_{3-j} (not D_j), so how should each agent choose to behave?

We can study this issue via game theory [Belmega-Sankar-Poor].

Rate and Privacy Leakage (Illustration)

$$\alpha = 1,\ \beta = 8,\ \sigma_1^2 = 0.05,\ \sigma_2^2 = 1$$



A One-Shot Game

The action a_j of agent j is the distortion caused at agent *3-j*, maximally $\bar{D}_{3-j}$.

A One-Shot Game

The action a_j of agent j is the distortion caused at agent $3\text{-}j$, maximally $\bar{D}_{3-j}$.

The payoff for agent j:

$$\boxed{u_j(a_j, a_{3-j}) = -w_j L(a_j) + w_j' \log\left(\frac{\bar{D}_j}{a_{3-j}}\right)}$$

A One-Shot Game

The action a_j of agent j is the distortion caused at agent *3-j*, maximally $\bar{D}_{3-j}$.

The payoff for agent *j*: $$\boxed{u_j(a_j, a_{3-j}) = -w_j L(a_j) + w_j' \log\left(\frac{\bar{D}_j}{a_{3-j}}\right)}$$

Nash equilibrium (prisoner's dilemma): $$\boxed{(a_1^*, a_2^*) = (\bar{D}_2, \bar{D}_1)}$$

A One-Shot Game

The action a_j of agent j is the distortion caused at agent $3\text{-}j$, maximally $\bar{D}_{3-j}$.

The payoff for agent j:

$$\boxed{u_j(a_j, a_{3-j}) = -w_j L(a_j) + w_j' \log\left(\frac{\bar{D}_j}{a_{3-j}}\right)}$$

Nash equilibrium (prisoner's dilemma):

$$\boxed{(a_1^*, a_2^*) = (\bar{D}_2, \bar{D}_1)}$$

Add pricing:

$$\boxed{\tilde{u}_j(a_j, a_{3-j}) = u_j(a_j, a_{3-j}) + p_j \log\left(\frac{\bar{D}_{3-j}}{a_j}\right)}$$

A One-Shot Game

The action a_j of agent j is the distortion caused at agent $3\text{-}j$, maximally $\bar{D}_{3-j}$.

The payoff for agent j:

$$u_j(a_j, a_{3-j}) = -w_j L(a_j) + w'_j \log\left(\frac{\bar{D}_j}{a_{3-j}}\right)$$

Nash equilibrium (prisoner's dilemma):

$$(a_1^*, a_2^*) = (\bar{D}_2, \bar{D}_1)$$

Add pricing:

$$\tilde{u}_j(a_j, a_{3-j}) = u_j(a_j, a_{3-j}) + p_j \log\left(\frac{\bar{D}_{3-j}}{a_j}\right)$$

Any behavior can then be incentivized within the limits of the model.

A Common-Goal Game

A common payoff:

$$u_{sys}(a_1, a_2) = -L(a_1) - L(a_2) + \frac{q}{2}\log\left(\frac{\bar{D}_1 + \bar{D}_2}{a_1 + a_2}\right)$$

A Common-Goal Game

A common payoff:

$$\boxed{u_{sys}(a_1, a_2) = -L(a_1) - L(a_2) + \frac{q}{2}\log\left(\frac{\bar{D}_1 + \bar{D}_2}{a_1 + a_2}\right)}$$

Enables cooperation in a non-cooperative setting (a potential game).

A Common-Goal Game

A common payoff:

$$\boxed{u_{sys}(a_1, a_2) = -L(a_1) - L(a_2) + \frac{q}{2}\log\left(\frac{\bar{D}_1 + \bar{D}_2}{a_1 + a_2}\right)}$$

Enables cooperation in a non-cooperative setting (a potential game).

Nontrivial equilibria exist; the nature of these depends on the value of q.

A Multi-Stage Game

T-stage game, with a discounted payoff for agent *j*:

$$\sum_{t=1}^{T} \rho^{t-1} u_j(a_j^{(t)}, a_{3-j}^{(t)})$$

A Multi-Stage Game

T-stage game, with a discounted payoff for agent *j*:

$$\sum_{t=1}^{T} \rho^{t-1} u_j(a_j^{(t)}, a_{3-j}^{(t)})$$

With $T < \infty$, the only Nash equilibrium (subgame perfect equilibrium):

$$(a_1^{(t)*}, a_2^{(t)*}) = (\bar{D}_2, \bar{D}_1), \forall t$$

A Multi-Stage Game

T-stage game, with a discounted payoff for agent *j*:

$$\sum_{t=1}^{T} \rho^{t-1} u_j(a_j^{(t)}, a_{3-j}^{(t)})$$

With $T < \infty$, the only Nash equilibrium (subgame perfect equilibrium):

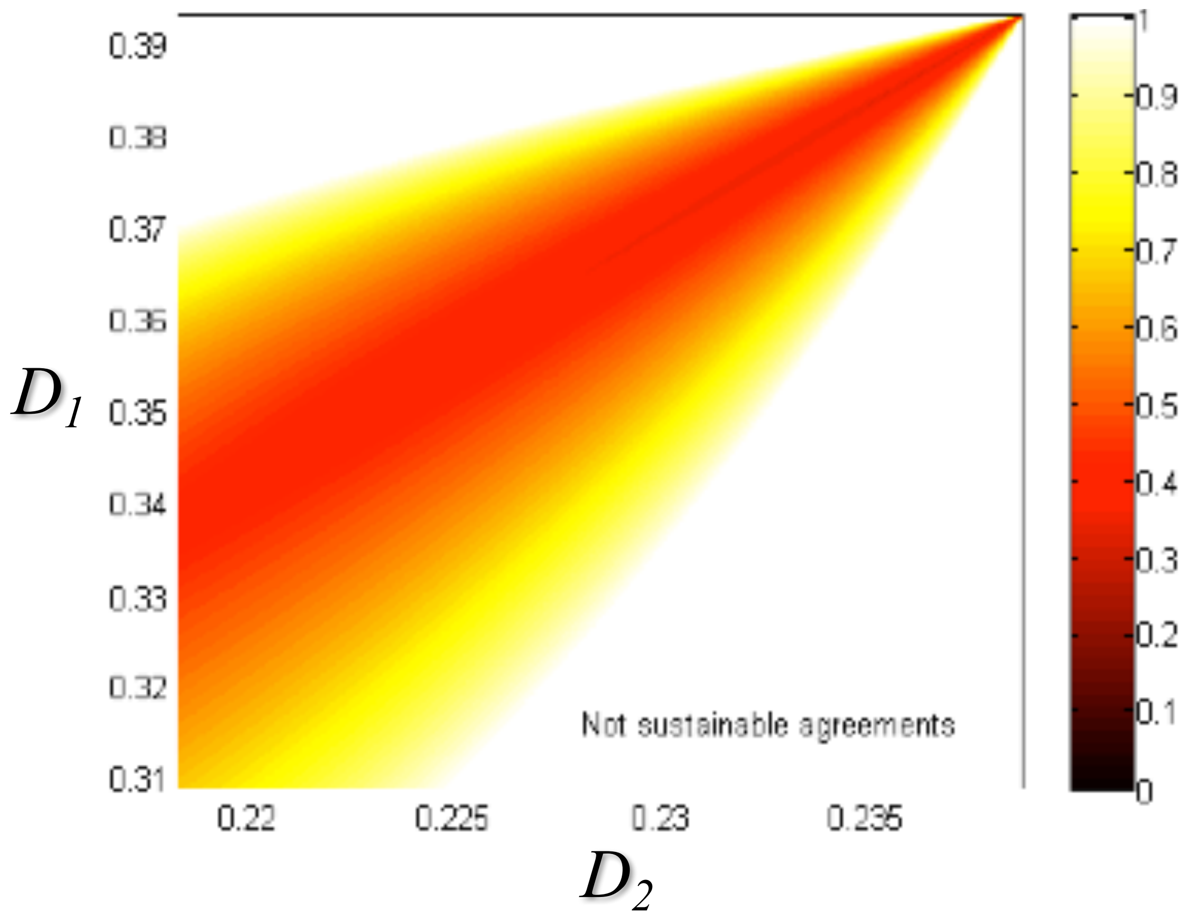
$$(a_1^{(t)*}, a_2^{(t)*}) = (\bar{D}_2, \bar{D}_1), \forall t$$

But, with $T = \infty$, any (D_1^*, D_2^*) satisfying the condition below is also a subgame perfect equilibrium for large enough $\rho < 1$:

$$u_j(D_j^*, D_{3-j}^*) > u_j(\bar{D}_j, \bar{D}_{3-j}); j = 1,2$$

Minimal Discount Factor for Sustaining Non-trivial Equilibria

$$\alpha = 0.9, \beta = 0.5, \sigma_1^2 = \sigma_2^2 = 0.1, w_j' = 5w_j$$



Summary (Competitive Privacy)

- An additional dimension to privacy vs. utility tradeoff is added when there are multiple competing agents.

Summary (Competitive Privacy)

- An additional dimension to privacy vs. utility tradeoff is added when there are multiple competing agents.
- Wyner-Ziv coding gives optimal information exchange.

Summary (Competitive Privacy)

- An additional dimension to privacy vs. utility tradeoff is added when there are multiple competing agents.
- Wyner-Ziv coding gives optimal information exchange.
- Game theory can help in modeling and understanding this problem:
  - one-shot games: prisoner's dilemma/pricing
  - multi-stage games: finite vs. infinite time window
  - common-goal games: enables cooperation

Summary

- Motivation: privacy-utility tradeoff

Summary

- Motivation: privacy-utility tradeoff
- General Formalism: information theoretic formulation

Summary

- Motivation: privacy-utility tradeoff
- General Formalism: information theoretic formulation
- Smart Meter Privacy: source coding & control approaches

Summary

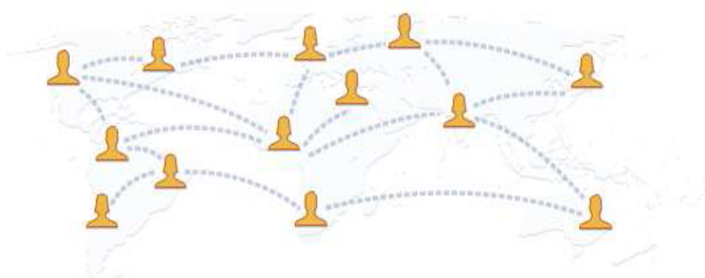
- Motivation: privacy-utility tradeoff
- General Formalism: information theoretic formulation
- Smart Meter Privacy: source coding & control approaches
- Competitive Privacy: game theoretic approach

Summary

- Motivation: privacy-utility tradeoff
- General Formalism: information theoretic formulation
- Smart Meter Privacy: source coding & control approaches
- Competitive Privacy: game theoretic approach
- Information-, control- and game-theoretic ideas allow fundamental examination of privacy issues in smart grid.

Basic P-U Tradeoff: Other Potential Applications

Biometric Systems: tradeoff between security & privacy



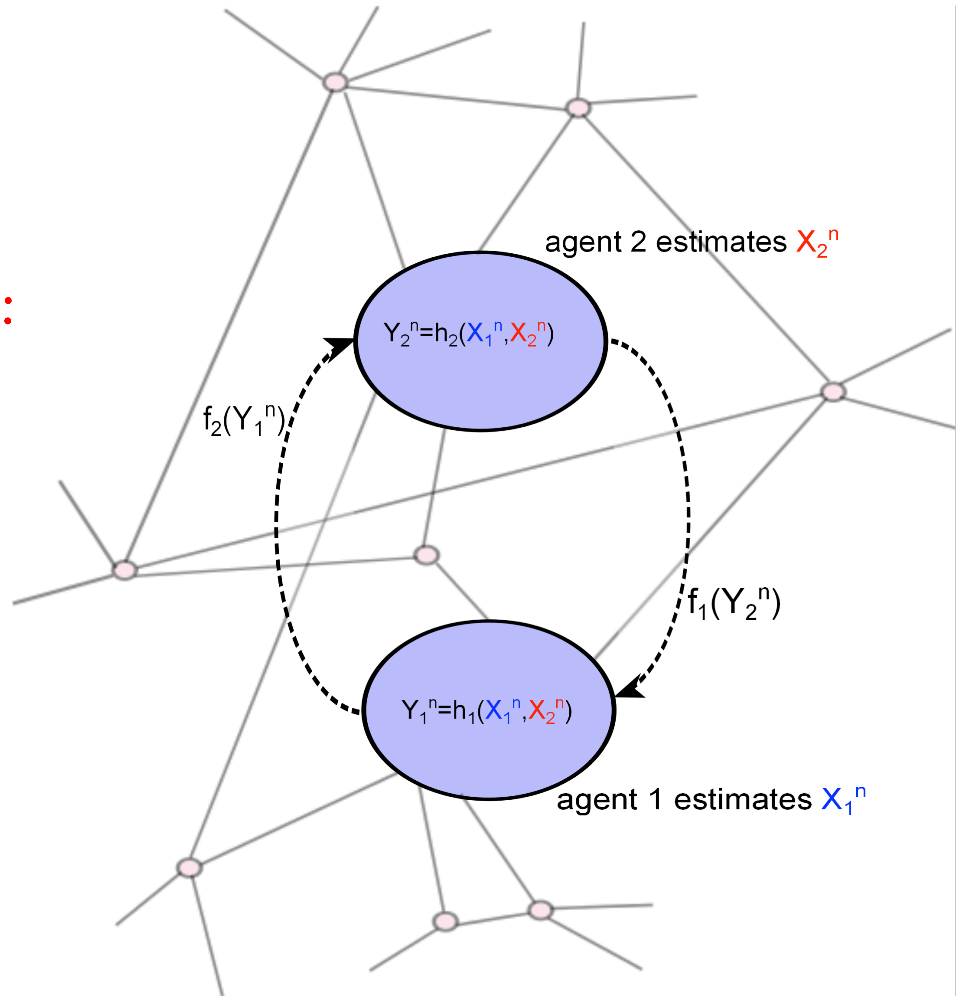
Social Networks: tradeoff between sharing & privacy

E-Commerce: tradeoff between economic benefit & privacy

Competitive Privacy: Other Potential Applications

Other Networks of Interacting Agents, e.g.:

- resource localization in competitive environments
- joint sensing with untrustworthy allies



References

S. Sankar, S. R. Rajagopalan, HVP, "Utility-Privacy Tradeoffs in Databases: An Information-theoretic Approach," *IEEE Trans. Inform. Forensics & Security* **8** (6) 838-852, 2013

S. Sankar, S. R. Rajagopalan, S. Mohajer, HVP, "Smart Meter Privacy: A Theoretical Framework," *IEEE Trans. Smart Grid* **4** (2) 837-846, 2013

O. Tan, D. Gündüz, HVP, "Increasing Smart Meter Privacy Through Energy Harvesting and Storage Devices," *IEEE JSAC: Smart Grid Communications* **31** (7) 1331-1341, 2013

L. Yang, X. Chen, J. Zhang, HVP, "Cost-Effective and Privacy-Preserving Energy Management for Smart Meters," *IEEE Trans. Smart Grid* **6** (1) 486-495, 2015

V. Belmega, L. Sankar, HVP, "Enabling Data Exchange in Interactive State Estimation under Privacy Constraints," *IEEE J. Select. Topics in Signal Process.* **9** (7) 1285-1297, 2015

HVP, "Privacy in the Smart Grid: Information, Control & Games," in *Information Theoretic Security and Privacy of Information Systems*. (Cambridge UP), to appear.

Thank you