Games, Privacy and Distributed Inference for the Smart Grid

Vince Poor
(poorg@princeton.edu)

Supported in part by NSF Grant CCF-1016671 and in part by the Marie Curie Outgoing Fellowship Program under Award No. FP7-PEOPLE-IOF-2011-298532.
Overview

Three Topics in Smart Grid:

Games, Privacy and Distributed Inference for the Smart Grid
Overview

Three Topics in Smart Grid:

- Game Theoretic Methods for Modeling Interactions
Overview

*Three Topics in Smart Grid:*

- *Game Theoretic Methods* for Modeling Interactions

- *Privacy-Utility Tradeoffs* for Data Sources
Overview

Three Topics in Smart Grid:

- Game Theoretic Methods for Modeling Interactions
- Privacy-Utility Tradeoffs for Data Sources
- Distributed Algorithms for State Estimation
Game Theoretic Methods for Modeling Interactions

Joint work with Walid Saad, et al.
Introduction & Motivation

• Salient characteristics of smart grid:
  
  - Heterogeneity: in terms of node types (electric vehicles, smart meters, substations, etc.) with each node having its own objective.
  
  - Large-scale interactions: spans large geographical areas and could incorporate thousands if not millions of nodes.
  
  - Stochastic dynamics: time-varying features, in terms of demand, supply, node dynamics (e.g., car mobility), etc.
Introduction & Motivation

- Salient characteristics of smart grid:
  - **Heterogeneity**: in terms of node types (electric vehicles, smart meters, substations, etc.) with each node having its own objective.
  - **Large-scale interactions**: spans large geographical areas and could incorporate thousands if not millions of nodes.
  - **Stochastic dynamics**: time-varying features, in terms of demand, supply, node dynamics (e.g., car mobility), etc.

- Need techniques that capture individual node objectives, large-scale interactions, and dynamics/uncertainty

---

Game Theoretic Methods for Modeling Interactions
Introduction & Motivation

- Salient characteristics of smart grid:
  - **Heterogeneity**: in terms of node types (electric vehicles, smart meters, substations, etc.) with each node having its own objective.
  - **Large-scale interactions**: spans large geographical areas and could incorporate thousands if not millions of nodes.
  - **Stochastic dynamics**: time-varying features, in terms of demand, supply, node dynamics (e.g., car mobility), etc.

- Need techniques that capture individual node objectives, large-scale interactions, and dynamics/uncertainty

- Useful framework - **game theory** in its two branches:
  - Non-cooperative game theory
  - Cooperative game theory

Game Theoretic Methods for Modeling Interactions
Introduction & Motivation

- Salient characteristics of smart grid:
  - **Heterogeneity**: in terms of node types (electric vehicles, smart meters, substations, etc.) with each node having its own objective.
  - **Large-scale interactions**: spans large geographical areas and could incorporate thousands if not millions of nodes.
  - **Stochastic dynamics**: time-varying features, in terms of demand, supply, node dynamics (e.g., car mobility), etc.

- Need techniques that capture individual node objectives, large-scale interactions, and dynamics/uncertainty

- Useful framework - **game theory** in its two branches:
  - Non-cooperative game theory
  - Cooperative game theory

- Illustrate via **two examples**

---

*Game Theoretic Methods for Modeling Interactions*
Groups of plug-in electric vehicles can trade energy with the main grid.
• Groups of plug-in electric vehicles can trade energy with the main grid.

• Non-cooperative games can model interactions among such groups.
Groups of plug-in electric vehicles can trade energy with the main grid.

Non-cooperative games can model interactions among such groups.

If the grid acts as a single entity, a Stackelberg (leader-follower) game provides a good model.
Ex. 1: Energy Trading for Plug-In Vehicles

- Groups of plug-in electric vehicles can trade energy with the main grid.

- Non-cooperative games can model interactions among such groups.

- If the grid acts as a single entity, a Stackelberg (leader-follower) game provides a good model.

- If grid elements act autonomously, a hybrid auction/Nash game can be used.

Game Theoretic Methods for Modeling Interactions
• Groups of plug-in electric vehicles can trade energy with the main grid.

• Non-cooperative games can model interactions among such groups.

• If the grid acts as a single entity, a Stackelberg (leader-follower) game provides a good model.

• If grid elements act autonomously, a hybrid auction/Nash game can be used. Consider this first, with the EV groups selling ...

Game Theoretic Methods for Modeling Interactions
Double Auction Market Model

[w/ Saad, Han, Basar – T-SG (submitted)]

- Double auction:
  - Order buyers by decreasing bids and sellers by increasing prices
  - Generate supply-demand curve

Game Theoretic Methods for Modeling Interactions
Double Auction Market Model

[w/ Saad, Han, Basar – T-SG (submitted)]

- Double auction:
  - Order buyers by decreasing bids and sellers by increasing prices
  - Generate supply-demand curve
  - Intersection: the aggregate demand and supply curve intersect at a point which determines:
    - The number and identity of the sellers and buyers that will trade; assume $L-1$ sellers and $M-1$ buyers trade

Game Theoretic Methods for Modeling Interactions
Double Auction Market Model

[w/ Saad, Han, Basar – T-SG (submitted)]

- Double auction:
  - Order buyers by decreasing bids and sellers by increasing prices
  - Generate supply-demand curve
  - Intersection: the aggregate demand and supply curve intersect at a point which determines:
    - The number and identity of the sellers and buyers that will trade; assume \( L-1 \) sellers and \( M-1 \) buyers trade
    - The trading price is given by

\[
\bar{p}(a) = \frac{s_L + b_M}{2}
\]

- \( a \) is the vector of energy put up for sale, \( s_L \) and \( b_M \) are the reservation bids of seller \( L \) and buyer \( M \)

Game Theoretic Methods for Modeling Interactions
A Non-Cooperative Game

[w/ Saad, Han, Basar – T-SG (submitted)]

- The strategy of a vehicle group $i$ is to choose the maximum amount $a_i$ of energy to sell.
The strategy of a vehicle group $i$ is to choose the maximum amount $a_i$ of energy to sell.

Vehicle group $i$ chooses its strategy to maximize its utility:

$$U_i(a_i, a_{-i}) = (\bar{p}(a) - s_i)Q_i(a) - \tau_i Q_i^2(a)$$

Trading price (auction outcome)  Quantity sold (auction outcome)  Pricing factor

Game Theoretic Methods for Modeling Interactions
The strategy of a vehicle group $i$ is to choose the maximum amount $a_i$ of energy to sell.

Vehicle group $i$ chooses its strategy to maximize its utility:

$$U_i(a_i, a_{-i}) = (\bar{p}(a) - s_i)Q_i(a) - \tau_i Q_i^2(a)$$

Trading price (auction outcome)  Quantity sold (auction outcome)  Pricing factor

How to solve the game and find the Nash equilibrium?

- Auction introduces a discontinuity => difficult analytically
- Algorithmic approach (based on best-response)

Game Theoretic Methods for Modeling Interactions
• Initially, the utility increases as more players enter the game leading to more energy sold.

• Then, the utility decreases as the presence of more sellers deflates the price.
Consider now the grid acting as a single entity (and selling to the vehicle groups).

Then we have a powerful leader (the grid) and less powerful (and competing) followers (the vehicle groups) - a Stackelberg game.

The utilities of the vehicle groups are still linear-quadratic in their strategies (i.e., how much they buy).

But, the price is set by the leader.

The leader’s utility is bi-linear = price × total quantity sold.

Leads to a Stackelberg equilibrium.

Game Theoretic Methods for Modeling Interactions
**Typical Simulation Results**

**Price vs. # Groups**

**Ave. Utility vs. # Groups**

*PSO = particle swarm optimization  
ED = equal distributions

*Game Theoretic Methods for Modeling Interactions*
Ex. 2: **Micro-grid Interaction**

[w/ Saad, Han– ICC’11]

- Energy trading within the distribution network

---

*Game Theoretic Methods for Modeling Interactions*


**Ex. 2: Micro-grid Interaction**

[w/ Saad, Han– ICC’11]

- Energy trading within the distribution network
- Cooperation helps to:
  - Exchange energy: sell surplus and overcome deficiency
  - Reduce power losses over transmission lines

---

*Game Theoretic Methods for Modeling Interactions*
Ex. 2: Micro-grid Interaction

[w/ Saad, Han– ICC’11]

- Energy trading within the distribution network
- Cooperation helps to:
  - Exchange energy: sell surplus and overcome deficiency
  - Reduce power losses over transmission lines
- Coalitional games

Game Theoretic Methods for Modeling Interactions
Coalition Games

- **Coalitional game** \((N,\nu)\)
  - In a set of players \(N\), a coalition \(S\) is a group of cooperating players
  - Value (utility) of a coalition \(\nu(S)\)
  - User payoff \(\phi_i(S)\): the portion received by a player \(i\) in a coalition \(S\)
Coalition Games

• **Coalitional game** \((N, v)\)
  
  - In a set of players \(N\), a *coalition* \(S\) is a group of cooperating players
  
  - **Value** (utility) of a coalition \(v(S)\)
  
  - **User payoff** \(\phi_i(S)\): the portion received by a player \(i\) in a coalition \(S\)

• **Coalition formation**
  
  - Coalitions can be compared based on **Pareto ordering** of user payoffs
  
  - **Merges and splits** can be used to iterate on coalitions
  
  - Convergence to a stable, **merge-and-split-proof limit**
For a coalition $S$, we define the value function as

$$v(S) = \max_{\pi \in \pi_S} u(S, \pi)$$

- The max is over all orderings of buyers & $u$ measures power losses.
- The utility represents a cost paid per unit of power loss.
For a coalition $S$, we define the value function as

$$v(S) = \max_{\pi \in \mathcal{T}_S} u(S, \pi)$$

- The max is over all orderings of buyers $\pi$ and $u$ measures power losses.
- The utility represents a cost paid per unit of power loss.

To divide the utility between the players, adopt a fair division proportional to the non-cooperative utility of each user:

$$\phi_i = \alpha_i \left( v(S) - \sum_{j \in S} v(\{j\}) \right) + v(\{i\}).$$

Weight chosen according to micro-grid $i$'s non-cooperative utility

$$\frac{\alpha_i}{\alpha_j} = \frac{v(\{i\})}{v(\{j\})} \quad \sum_{i \in S} \alpha_i = 1.$$
- Emergence of local markets
- Here, we see a single snapshot; it is of interest for future work to see how this evolves as demand/supply vary
Typical Simulation Results (2)

Game Theoretic Methods for Modeling Interactions
Summary

• Game theory for smart grid modeling:
  – Demand-side management, energy trading and markets
  – Integration and distributed operation of micro-grids
  – “Game theoretic methods for the smart grid,” [w/ Saad, Han, Basar - SPM’12]
Summary

• Game theory for smart grid modeling:
  – Demand-side management, energy trading and markets
  – Integration and distributed operation of micro-grids
  – “Game theoretic methods for the smart grid,” [w/ Saad, Han, Basar - SPM’12]

• Other problems of interest
  – Network formation games for PLC backhaul [w/ Saad, Han - Gamenets’11]
  – Social optimality of equilibria in trading markets [w/ Tushar, et al. – ICC’13]
Summary

- **Game theory for smart grid modeling:**
  - Demand-side management, energy trading and markets
  - Integration and distributed operation of micro-grids
  - “Game theoretic methods for the smart grid,” [w/ Saad, Han, Basar - SPM’12]

- **Other problems of interest**
  - Network formation games for PLC backhaul [w/ Saad, Han - Gamenets’11]
  - Social optimality of equilibria in trading markets [w/ Tushar, et al. – ICC’13]

- **Additional issues**
  - Optimizing jointly over three layers: economic, cyber, and physical
  - Incorporating dynamics (generation/load/mobility/etc.)

*Game Theoretic Methods for Modeling Interactions*
Privacy-Utility Tradeoffs for Data Sources

Joint work with Lalitha Sankar, et al.

Games, Privacy and Distributed Inference for the Smart Grid
Motivation: The Privacy Problem

- There are many electronic information sources of information about us.
  - Google, Facebook, smart metering, etc.
• There are many electronic information sources of information about us.
  – Google, Facebook, smart metering, etc.

• The utility of these sources depends on their accessibility.

Privacy-Utility Tradeoffs for Data Sources
There are many electronic information sources of information about us.

- Google, Facebook, smart metering, etc.

The utility of these sources depends on their accessibility.

But, they can also leak private information.
Motivation: The Privacy Problem

- There are many electronic information sources of information about us.
  - Google, Facebook, smart metering, etc.

- The utility of these sources depends on their accessibility.
- But, they can also leak private information.
- How can we characterize this fundamental tradeoff?

Privacy-Utility Tradeoffs for Data Sources
A database is a table – rows: individual entries (total of $n$); columns: attributes for each individual (total of $K$).

**Database Model**

- **Attributes**
- **Entries**

```
+----------------+----------------+----------------+--------+
| Gender         | Visit Date     | Diagnosis      | ...    |
+----------------+----------------+----------------+--------+
| 1              |                |                |        |
| 2              |                |                |        |
| ...            |                |                |        |
| $n$            |                |                |        |
+----------------+----------------+----------------+--------+
```

**Privacy-Utility Tradeoffs for Data Sources**
Database: Source Model

- Database with \( n \) rows is 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:

\[
p_X(\mathbf{x}) = p_{X_1 X_2 \ldots X_K}(x_1, x_2, \ldots, x_K)
\]
Database: Source Model

- Database with $n$ rows is 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:

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

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

$$X_{r,k} : \text{revealed} \quad \longrightarrow \quad X_{h,k} : \text{hidden} \quad \rightarrow \quad k^{th} \text{ entry: } \mathbf{X}_k = (X_{r,k}, X_{h,k})$$

Privacy-Utility Tradeoffs for Data Sources
Privacy-Utility Tradeoff

[w/ Sankar, Rajagapolan - T-IFS’13]

• Contrast between privacy and secrecy:
Privacy-Utility Tradeoff

[w/ Sankar, Rajagapolan - T-IFS’13]

• Contrast between privacy and secrecy:
  – In the (communications) secrecy problem, there is a single source with legitimate and eavesdropping receivers.
Privacy-Utility Tradeoff

[w/ Sankar, Rajagapolan - T-IFS’13]

• Contrast between privacy and secrecy:

  – In the (communications) secrecy problem, there is a single source with legitimate and eavesdropping receivers.

  – In the privacy problem, we have a single “receiver” (the query initiator) with the source being divided into private and public variables.
Privacy-Utility Tradeoff

[w/ Sankar, Rajagapolan - T-IFS’13]

• Contrast between privacy and secrecy:

  – In the (communications) secrecy problem, there is a single source with legitimate and eavesdropping receivers.

  – In the privacy problem, we have a single “receiver” (the query initiator) with the source being divided into private and public variables.

• How can we characterize the tradeoff between utility and privacy in such a setting?
• Contrast between privacy and secrecy:
  
  – In the (communications) secrecy problem, there is a single source with legitimate and eavesdropping receivers.
  
  – In the privacy problem, we have a single “receiver” (the query initiator) with the source being divided into private and public variables.

• How can we characterize the tradeoff between utility and privacy in such a setting?
  
  – Measure utility by distortion of the public variables as revealed to a user of the database;
Privacy-Utility Tradeoff

[w/ Sankar, Rajagapolan - T-IFS’13]

• Contrast between privacy and secrecy:

  – In the (communications) secrecy problem, there is a single source with legitimate and eavesdropping receivers.

  – In the privacy problem, we have a single “receiver” (the query initiator) with the source being divided into private and public variables.

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

  – Measure utility by distortion of the public variables as revealed to a user of the database; and

  – Measure privacy by equivocation on the private variables in information revealed to a user.
Contrast between privacy and secrecy:

- In the (communications) secrecy problem, there is a single source with legitimate and eavesdropping receivers.
- In the privacy problem, we have a single “receiver” (the query initiator) with the source being divided into private and public variables.

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

- Measure utility by distortion of the public variables as revealed to a user of the database; and
- Measure privacy by equivocation on the private variables in information revealed to a user.

Then the distortion-equivocation region describes the tradeoff.
**Distortion-Equivocation Model**

[w/ Sankar, Rajagapolan - T-IFS’13]

- Encoder maps the original database to a “sanitized” database (SDB):

\[
\text{Encoder} : X^n \rightarrow \mathcal{W} = \{SDB_1, SDB_2, \ldots, SDB_M\}
\]

Privacy-Utility Tradeoffs for Data Sources
Distortion-Equivocation Model

[w/ Sankar, Rajagopolan - T-IFS’13]

- Encoder maps the original database to a “sanitized” database (SDB):

\[
\text{Encoder} : \mathbf{X}^n \rightarrow \mathcal{W} = \{ \text{SDB}_1, \text{SDB}_2, \ldots, \text{SDB}_M \}
\]

Privacy-Utility Tradeoffs for Data Sources
**Distortion-Equivocation Model**

[w/ Sankar, Rajagapolan - T-IFS’13]

- Encoder maps the original database to a “sanitized” database (SDB):

\[
\text{Encoder} : X^n \rightarrow \mathcal{W} = \{SDB_1, SDB_2, \ldots, SDB_M\}
\]

**Distortion**

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

**Diagram:**

Source \(\{X_{r,k}, X_{h,k}\}_{k=1}^{n}\) \(\rightarrow\) Encoder \(\rightarrow\) Decoder \(\{\tilde{X}_{r,k}\}_{k=1}^{n}\)  

**Privacy-Utility Tradeoffs for Data Sources**
**Distortion-Equivocation Model**

[w/ Sankar, Rajagapolan - T-IFS’13]

- Encoder maps the original database to a “sanitized” database (SDB):

  \[\text{Encoder} : X^n \rightarrow \mathcal{W} = \{SDB_1, SDB_2, \ldots, SDB_M\}\]

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

\[\Delta_p \equiv \frac{1}{n} H(X^n_h | W) > E - \varepsilon\]

Privacy-Utility Tradeoffs for Data Sources
Distortion-Equivocation Model

Encoder maps the original database to a “sanitized” database (SDB):

Encoder: \( \mathbf{X}^n \rightarrow \mathcal{W} = \{SDB_1, SDB_2, \ldots, SDB_M\} \)

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

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

Source \( \left\{ \mathbf{X}_{r,k}, \mathbf{X}_{h,k} \right\}_{k=1}^{n} \) \rightarrow Encoder \( W \in \mathcal{W} \) \rightarrow Decoder \( \left\{ \tilde{\mathbf{X}}_{r,k} \right\}_{k=1}^{n} \)

Add a rate constraint \( M \leq 2^{n(R+\varepsilon)} \)

Privacy-Utility Tradeoffs for Data Sources
Utility-Privacy/RDE Regions

Our Approach: Utility-Privacy Tradeoff Region
Privacy-exclusive Region (current art)
Privacy-indifferent Region

(a): Rate-Distortion-Equivocation Region
Feasible Distortion-Equivocation region $R_{D,E}$.

(b): Utility-Privacy Tradeoff Region

Privacy-Utility Tradeoffs for Data Sources
Competitive Privacy

- N.A. Grid: interconnected regional transmission organizations (RTOs) which
  - need to share measurements on state estimation for reliability (utility)
N.A. Grid: interconnected regional transmission organizations (RTOs) which
- need to share measurements on state estimation for reliability (utility)
- wish to withhold information for economic competitive reasons (privacy)
**Competitive Privacy**

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

- Leads to a problem of **competitive privacy**
Competitive Privacy

[w /Sankar, Kar - Asilomar’12]

- Noisy measurements at RTO k:

\[ Y_k = \sum_{m=1}^{M} H_{k,m} X_m + Z_k, \quad k = 1, 2, \ldots, M \]
Competitive Privacy

[w/Sankar, Kar - Asilomar'12]

- Noisy measurements at RTO $k$:

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

- Utility for RTO $k$: mean-square error for its own state $X_k$
**Competitive Privacy**

[w /Sankar, Kar - Asilomar’12]

- Noisy measurements at RTO k:

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

- 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

*Privacy-Utility Tradeoffs for Data Sources*
Competitive Privacy

[w /Sankar, Kar - Asilomar‘12]

- Noisy measurements at RTO $k$:

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

- 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

Wyner-Ziv coding maximizes privacy for a desired utility at each RTO.
Smart Meter Privacy

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

- Smart meter data is useful for price-aware usage, load balancing
- But, it leaks information about in-home activity
P-U tradeoff leads to a spectral ‘reverse water-filling’ solution
P-U tradeoff leads to a spectral ‘reverse water-filling’ solution
P-U tradeoff leads to a spectral ‘reverse water-filling’ solution.

Can also use energy storage to aid privacy [w/ Tan, Gunduz, JSAC:SG Series’13]

Privacy-Utility Tradeoffs for Data Sources
Summary

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

Privacy-Utility Tradeoffs for Data Sources
Summary

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

• Applications in smart grid include: competitive privacy & smart metering
Summary

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

• Applications in smart grid include: competitive privacy & smart metering

• Can also consider
  • multiple queries (successive disclosure)
  • multiple sources (side information)
Distributed Algorithms for State Estimation

Joint work with Le Xie, et al.

Games, Privacy and Distributed Inference for the Smart Grid
• Computational & communications challenge:
  - fast sensing (e.g., Phasor Measurement Units) produces big data, and communications bottlenecks

• Restructuring/deregulation means more RTOs, or control areas (CAs)

• Situational awareness needed for large interconnected power systems:
  - wide area monitoring, control and protection (WAMCP)

• Of interest: a distributed estimation framework to obtain the system-wide states through information exchange among CAs.

*Motivation*

*Distributed Algorithms for State Estimation*
Proposed Solution

Wide area state estimation via distributed iterative information processing:

Key Properties

- No central coordinator
- Only *local information* (measurement Jacobian matrix, measurement vector) required
- All local control areas *not necessarily* observable
- Flexible in communication topology
- Equivalent performance to centralized approach

Conceptual Model

*Distributed Algorithms for State Estimation*
Distributed Measurement Model

• **System State**
  
  \[ \theta \in \mathbb{R}^M : \text{The network system state (vector) consisting of voltage phase angles of buses in all CAs.} \]

• **CA Local Observation Model**

  \[ z_n \in \mathbb{R}^{M_n} : \text{The local observation at CA } n \]

  \[ z_n = H_n \theta + e_n, \]

  where the Jacobian \( H_n \in \mathbb{R}^{M_n} \) sub-block represents the local physical interconnections.

Distributed Algorithms for State Estimation
Proposed Distributed Iterative Solution

Each CA $n$ has only local knowledge of the network structure and measurements and updates a local estimate $x_n$ as follows:

$$x_n(t + 1) = x_n(t) - \beta_t \sum_{l \in \Omega_n} (x_n(t) - x_l(t)) + \alpha_t \overline{H}_n^T (\overline{z}_n - \overline{H}_n x_n(t)),$$

where

- $\Omega_n$: communication neighborhood of CA $n$
- $\overline{H}_n = R_n^{-1/2} H_n$
- $\overline{z}_n = R_n^{-1/2} z_n$

Distributed Algorithms for State Estimation
Global observability of the grid (i.e., $\sum_{n=1}^{N} H_n^T H_n$ is full rank)

+ connectivity of the communication network (i.e. the second smallest eigenvalue of the graph Laplacian is positive) ...

assures a.s. convergence of local estimates to the global estimate (least squares with all measurements) with appropriately programmed $\alpha$’s and $\beta$’s.
Test Bus Systems

- Overall systems are globally observable
- CAs are globally unobservable
- Shaded CAs are locally unobservable

Distributed Algorithms for State Estimation
Convergence of Phase Estimates

14-Bus System

118-Bus System

Distributed Algorithms for State Estimation
Communication Topology Flexibility

14-Bus System

Distributed Algorithms for State Estimation
Related Work

- **Nonlinear (AC) state estimation** [w/ Xie, Choi, Kar, T-SG’12]

- **Multi-cast routing** [w/ Li, Lai, JSAC:SG Series’12]

- **Games** for privacy-aware distributed state estimation [w/ Belmega, Sankar – NetGCoop’12 & T-SG (submitted)]

Distributed Algorithms for State Estimation
Summary

Three Topics in Smart Grid:

- **Game Theoretic Methods** for Modeling Interactions
- **Privacy-Utility Tradeoffs** for Data Sources
- **Distributed Algorithms** for State Estimation
Thank You!