A Framework for the Impact Analysis of Data Quality/Integrity/Privacy in Cyber-Physical Electric Energy System

ELECTRICAL & COMPUTER ENGINEERING
TEXAS A&M UNIVERSITY

Dae-Hyun Choi (cdh8954@neo.tamu.edu) and Le Xie (Lxie@ece.tamu.edu)

Motivation

- **Emergence of heterogeneous multi-scale spatial sensor data in cyber-physical electric energy systems**
  - Synchrophasor data (transmission level)
  - Smart meter data (distribution level)
- **Smart grid cyber security and privacy**
  - Data integrity attack on physical and economical grid operations [1], [2]
  - Violation of consumer privacy by monitoring energy usage data maliciously [3]
- Need for **novel frameworks** and **algorithms** to analyze and design **robust cyber-physical electric energy systems** against bad/malicious multi-scale spatial data

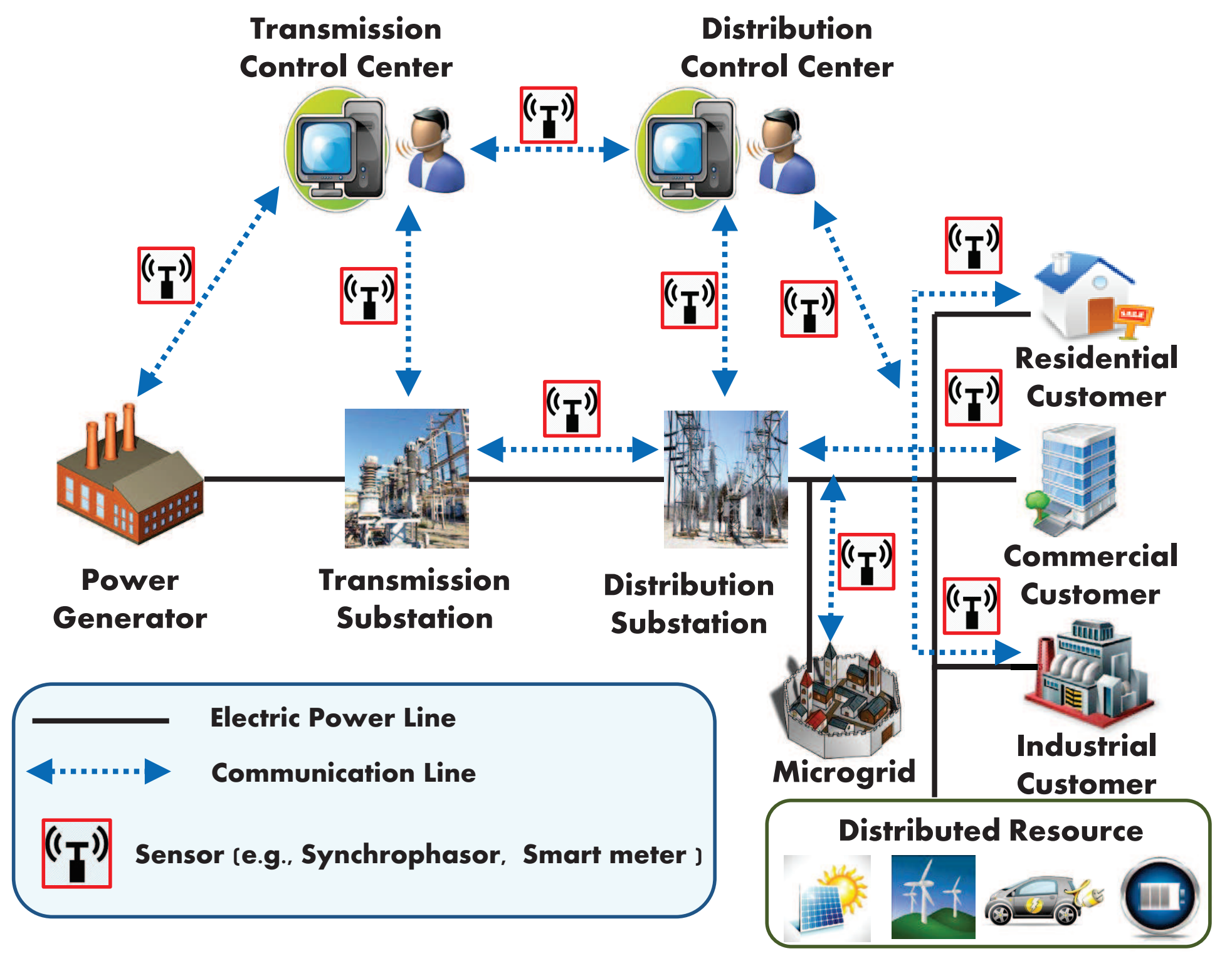


Figure 1: Smart grid operations based on advanced grid sensor data

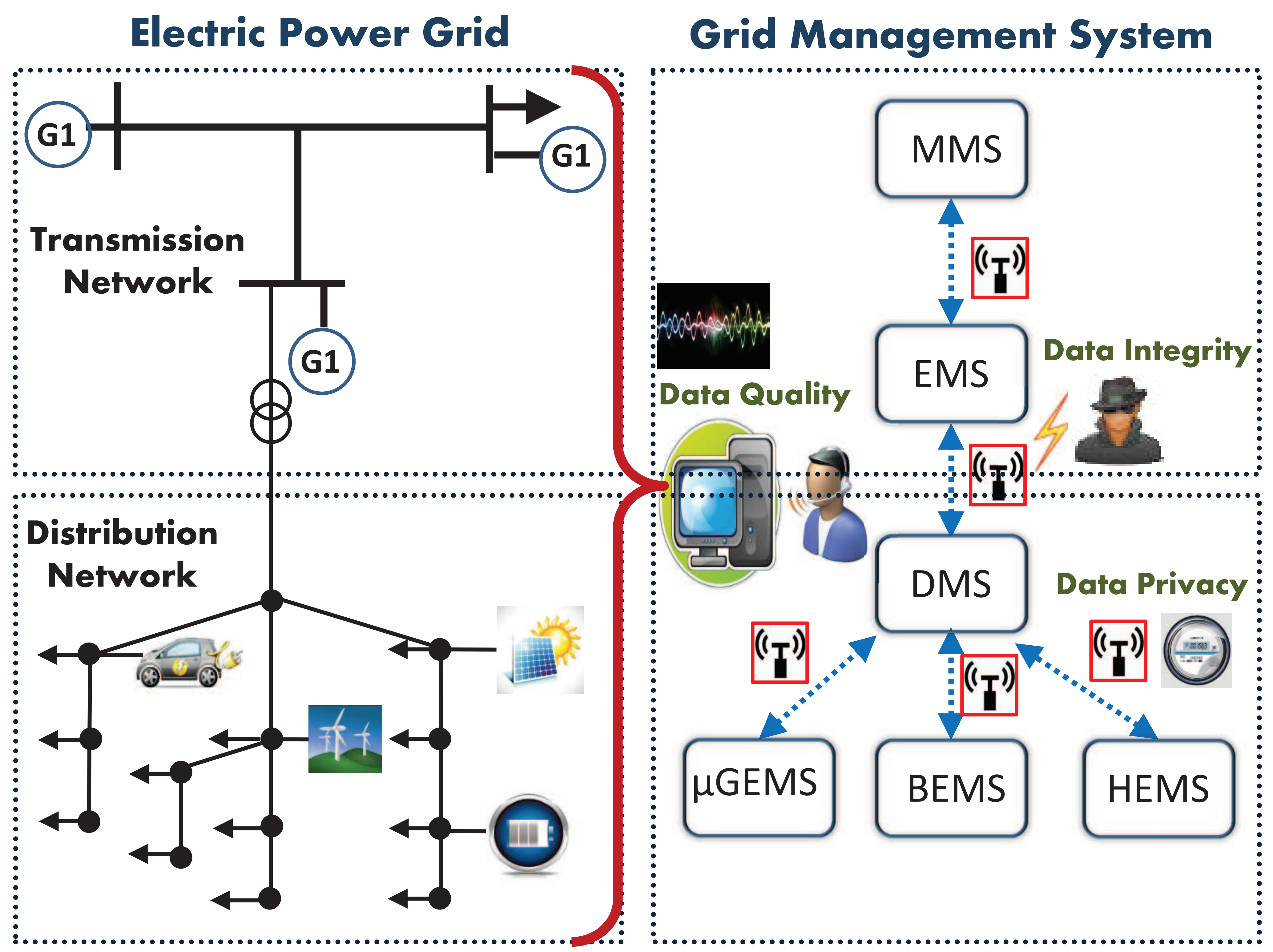
Proposed Research Goals

The proposed research is conducted along the following directions related to (1) **data quality**, (2) **data integrity** and (3) **data privacy**:

(a) develop a unified system-wide monitoring tool for multi-scale spatial grid **data quality** analysis

(b) create a resilient multi-area state estimation architecture and sensing/communication system to mitigate the risk of **data integrity** attack

(c) develop a novel **data privacy**-preserving algorithm and infrastructure to prevent malicious energy consumption monitoring



* EMS/MMS: Energy/Market Management System, DMS: Distribution Management System

* μGEMS/BEMS/HEMS: Micro Grid/Building/Home Energy Management System

Figure 2: Multi-Scale Spatial Model for Electric Power Grid and Grid Management System

Data Quality-Aware Multi-Scale Decision Making

Goal: development of a unified framework for multi-scale spatial data quality analysis

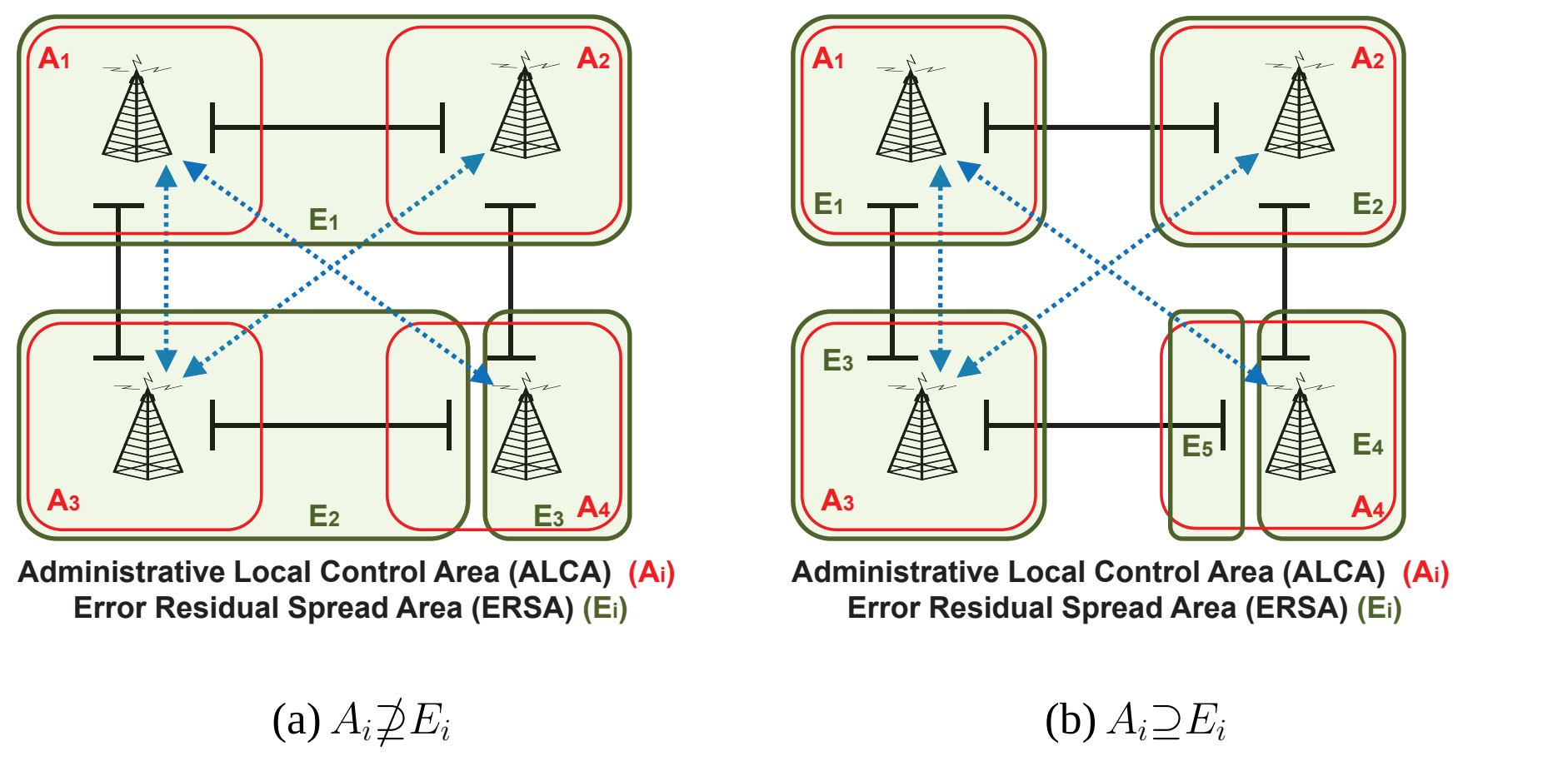
- Design of interface between heterogeneous grid management systems
  - Definition of exchanged data type
- Proposal of performance metric to assess multi-scale spatial data quality
  - E.g., three-level KKT condition perturbation approach-based sensitivity matrix $\mathcal{S}$:

$$\mathcal{S} = \frac{\partial \pi_{\mathrm{MMS}}}{\partial \mathbf{z}_{\mathrm{DATA}}} = \frac{\partial \pi_{\mathrm{MMS}}}{\partial \hat{\mathbf{x}}_{\mathrm{EMS}}} \cdot \frac{\partial \hat{\mathbf{x}}_{\mathrm{EMS}}}{\partial \hat{\mathbf{y}}_{\mathrm{DMS}}} \cdot \frac{\partial \hat{\mathbf{y}}_{\mathrm{DMS}}}{\partial \mathbf{z}_{\mathrm{DATA}}}$$

▶ π_{MMS}: state variable in MMS
▶ $\hat{\mathbf{x}}_{\mathrm{EMS}}$: (estimated) state variable in EMS
▶ $\hat{\mathbf{y}}_{\mathrm{DMS}}$: (estimated) state variable in DMS
▶ $\mathbf{z}_{\mathrm{DATA}}$: sensor data for DMS

Data Integrity-Resilient Power System State Estimation

Goal: development of attack-resilient multi-area state estimation


A1
A2
A3
A4
E1
E2
E3
A1
A2
A3
A4
E1
E2
E3
E4
E5
Administrative Local Control Area (ALCA) (Ai)
Error Residual Spread Area (ERSA) (Ei)
Administrative Local Control Area (ALCA) (Ai)
Error Residual Spread Area (ERSA) (Ei)

(a) $A_i \not\supseteq E_i$

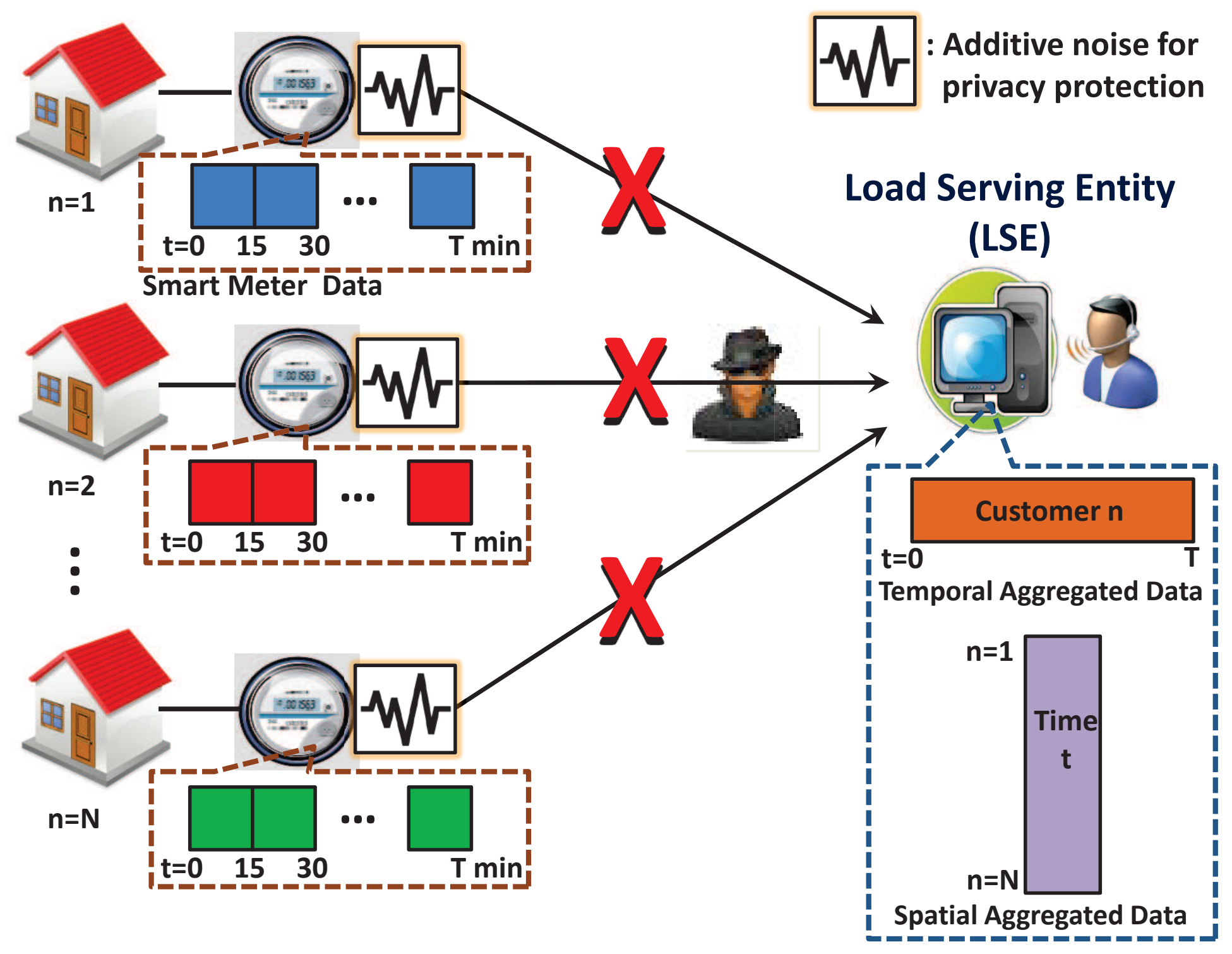
(b) $A_i \supseteq E_i$

(a) **ALCA does not overlap ERSA**
False data in A_4 affects the residuals in A_3
→ malfunction of bad data detection in A_3

(b) **ALCA completely includes ERSA**
False data in A_4 are localized in E_4,$E_5 \subseteq A_4$
→ **a novel sensor placement strategy** required

Data Privacy-Preserving Model for Smart Metering

Goal: design of privacy protocol and algorithm for smart metering



- Additive noise-based statistical smart metering model for data privacy (e.g., Gaussian mixture model)
- Development of method for LSE' estimating spatial and temporal aggregated energy consumption from corrupted meter data

Potential Impact on CPS

Reliable, economical and secure cyber-physical electric energy systems can be analyzed and operated by the proposed frameworks and algorithms:

- A unified system-wide monitoring and visualization tool on the level of multi-scale spatial data quality
- Architecture and algorithms to detect potential cyber data integrity attacks and protect consumer's data privacy from malicious monitoring

Key References

[1] D.-H. Choi and L. Xie, "Ramp-induced Data Attacks on Look-ahead Dispatch in Real-time Power Markets," *IEEE Trans. Smart Grid.*, vol. 4, no. 3, pp. 1235-1243, Sept 2013.

[2] D.-H. Choi and L. Xie, "Sensitivity Analysis of Real-Time Locational Marginal Price to SCADA Sensor Data Corruption," *IEEE Trans. Power Syst.* (accepted,to appear)

[3] S. Wang, L. Cui, J. Que, D.-H. Choi, X. Jiang, S. Cheng, and L. Xie, "A Randomized Response Model for Privacy Preserving Smart Metering," *IEEE Trans. Smart Grid.*, vol. 3, no. 3, pp. 1317-1324, Sept 2012.