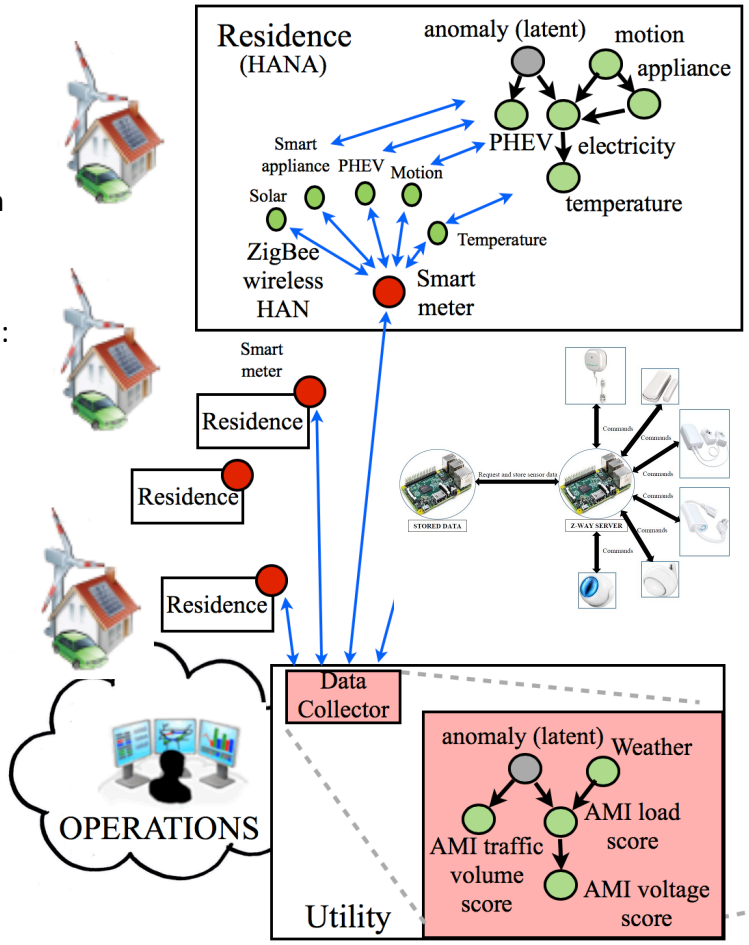
Integrated Smart Grid Analytics for Anomaly Detection

Challenge:

- **Threat model**: false data injection attacks. Power grid not isolated anymore due to AMI's two-way communication capabilities
- Orchestrated bad data injection attacks that suddenly elevate power demand **can destabilize the power grid**
- Known ICS /SCADA case studies: Stuxnet, attack on Ukrainian power grid, German steel mill

Solution:

- Data-driven situation awareness
- Correlative monitoring
- **Home-area networks**: monitor features that affect electricity consumption (motion within house, temperature, luminosity). Predict consumption & Detect anomalies. TTP prototype in-place
- **Wide-area networks**: statistical network-kriging approach. Predict consumption of "unsecure" buildings, using secure smart meters



Scientific Impact:

- Behavioral-based anomaly detection from home-area vantage point is a novel method for tracking smart meter anomalies
- Study of efficient, adaptive algorithms that capture temporal and spatial aspects of energy consumption

Broader Impact:

- Reliable operation of the smart power grid
- **Transition to practice**: prototype in place at NextEnergy in Detroit. In-expensive, off-the-shelf hardware based on Raspberry Pi's and ZWave sensors
- Education and Outreach: project lies at the intersection of computer science, statistics and engineering. Helped trained several undergraduate students participating at UM's Undergraduate Research Opportunity Program

Project info: CNS-1422078, University of Michigan / Merit Network, Dr. Joe Adams, Dr. Michael Kallitsis, University of Florida, Prof. George Michailidis