Integrated Smart Grid Analytics for Anomaly Detection

PIs: Michael Kallitsis (Umich,Merit), George Michailidis (UF), Samir Tout (EMU), William Adams (Umich,Merit)

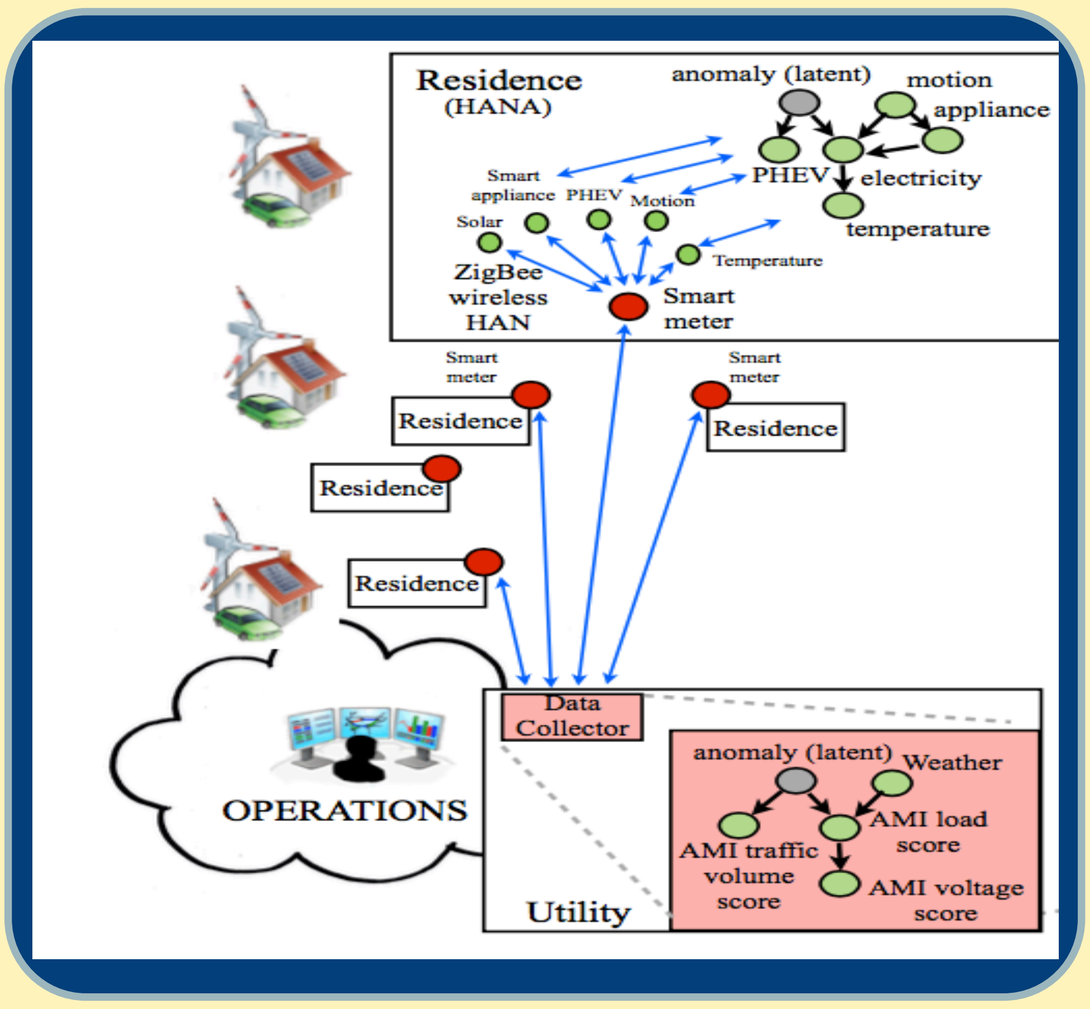
Main Project Repository: https://github.com/Merit-Research/Sensor-Polling

Staging TTP Repository: https://github.com/samemu/TTP-Dev

Anomaly Detection Using Hierarchical & Correlative Monitoring

The objective of this project is to detect potential anomalies, caused by nefarious activities in the modern Smart Grid's data plane. This study will increase the security of the Smart Grid and help enhance its future design decisions.

The Smart Grid uses the Advanced Metering Infrastructure (AMI), which employs real-time messaging to support its demand-response schemes. This exposes the entire grid to security threats, such as spoofed payload content that would lead to incorrect assessment of actual demand.



Nefarious data plane activities can compromise grid stability, reliability and efficiency. Hence, it is important to ensure secure communications and quickly detect malicious activity. Real-world security incidents on ICS/SCADA networks include: a) Stuxnet worm, b) Ukrainian power grid, c) German steel mill

Correlative Monitoring Approach

- Forecasting Module
  - Prediction using Bayesian Linear Regression, Neural Networks, etc.
- Compare predicted vs. actual smart meter reading
  - Sequential hypothesis testing: Sequence of abnormally small p-values

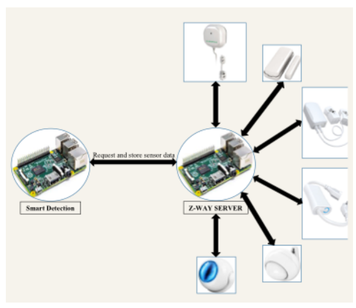
Framework 1 Measurement-based False Data Detection

Require: For each forecasting period: new training set $\mathbf{X}$ and $\mathbf{t}$.
Require: Control chart parameters λ and L.
Require: Robust threshold θ_r and period ν.
1: [Start] Fit the model and begin data monitoring.
2: [Forecast] Upon observing $(t_n, \mathbf{x}_n)$, compute $y(\mathbf{x}_n, \mathbf{w})$.
3: [Update] Compute error $e_n = t_n - y(\mathbf{x}_n, \mathbf{w})$.
4: [Control Chart] Compute $S_n = f(\lambda, L, e_n)$.
5: [Robust EWMA] Apply two-in-a-row rule on S_n (see section III-B).
6: [Robust Filter] Update $A = \{k : |S_k| > L\sigma_\lambda, k = n - \nu, \ldots, n\}$.
7: [Decision] Raise alarm if $|A| > \theta_r$, else system is in-control.

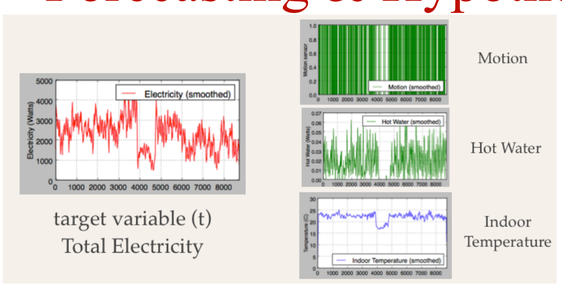
A practical system for HAN Monitoring

Data Collection → Forecasting → Hypothesis Testing → Dashboard/ App

- Data-driven methodology
- Associate AMI energy consumption with data from sensors & Raspberry Pi's
- Sensor examples: motion, temperature, circuit info, etc.
- Off-the-shelf Zwave sensors for home automation



Forecasting & Hypothesis Testing



- ***Forecasting/Predictive Model***
  - Forecast energy consumption: past (training window) + other sensor readings
  - Upon observing (t_n, x_n), comp. $y(x_n, w)$
  - Compute forecasting error: $e_n = t_n - y(x_n, w)$
- ***Hypothesis Testing:***
  - Use *predictive distribution* to calculate tail (p-value) of error
  - Use EWMA to identify out of control

Transition to Practice: NextEnergy Home

- Successful collection of data from NextEnergy Smart Home
- Successful tests with Smart* Dataset with random injections

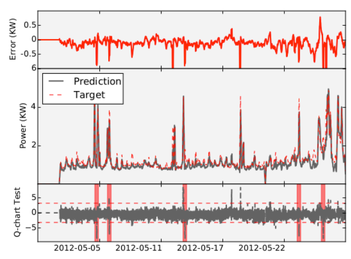


TABLE I: Evaluation of detection performance on the Smart* dataset. Values in parenthesis signify standard deviations.

Shift (KW)	Weight λ	Delay (in mins)	Precision	Recall	F1-score
−1	1	$9.7_{(7.2)}$	$.29_{(.45)}$	$.07_{(.11)}$	.11
−1	.53	$8.1_{(4.6)}$	$.76_{(.41)}$	$.29_{(.21)}$	.42
−1	.84	$10.4_{(5.5)}$	$.48_{(.50)}$	$.12_{(.14)}$	.19
1	1	$8.0_{(4.5)}$	$.75_{(.43)}$	$.26_{(.19)}$	.38
1	.53	$3.4_{(1.7)}$	$.95_{(.17)}$	$.50_{(.22)}$	.66
1	.84	$6.6_{(3.4)}$	$.86_{(.31)}$	$.31_{(.19)}$	.46
3	1	$1.1_{(.5)}$	$.98_{(.05)}$	$1.00_{(.03)}$	.99
3	.53	$1.0_{(.0)}$	$.98_{(.06)}$	$1.00_{(.03)}$	.99
3	.84	$1.0_{(.2)}$	$.98_{(.06)}$	$1.00_{(.03)}$	.99
6	1	$1.2_{(.9)}$	$.96_{(.11)}$	$.99_{(.05)}$	.97
6	.53	$1.0_{(.0)}$	$.97_{(.08)}$	$1.00_{(.05)}$	.98
6	.84	$1.0_{(0.0)}$	$.96_{(.09)}$	$.99_{(.05)}$	.98

Wide-Area Network Monitoring

- **Real-world data:** building power consumption data
- 160 buildings at University of Michigan for 2015
- **Network kriging** approach: statistical prediction of smart meter electricity consumption, based on others' observations in network
- *Adaptive Statistical Detection of False Data Injection Attacks in Smart Grids", by M. Kallitsis, S. A. Stoev, S. Bhattacharya, and G. Michailidis., IEEE GlobalSIP 2016, Washington, DC, Dec. 2016.*
- *Correlative Monitoring for Detection of False Data Injection Attacks in Smart Grids", by Kallitsis, M., Michailidis, G., and Tout, S., Proceedings of the IEEE SmartGridComm Conference, Miami, Florida, S2-4, Nov 2015.*

Acknowledgement of Students & Partners: Yeabsera Kebede, Atman Fozdar, Adrian Padin, Richard Kalvaitis, Davis Vorva, Nikolas Remley, Max Morgan; NextEnergy: Wayne Snyder

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Secure and Trustworthy Cyberspace
Inaugural Principal Investigator Meeting
Nov. 27 -29th 2012
National Harbor, MD