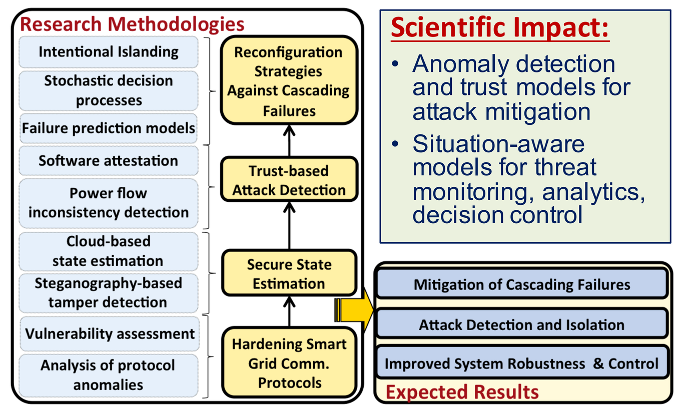
CPS: Breakthrough: Securing Smart Grid by Understanding Communications Infrastructure Dependencies

CNS-1544904 (K. Kant , Temple University), CNS-1545037 (S. K. Das, S. Silvestri, M. Crow, Missouri S&T)

Overview

Objectives:

- Characterize inter-dependence between electrical grid and communication systems
- Secure protocols for state estimation more robust in transmission and distribution network.
- Assure Data Integrity from Advanced metering infrastructure and customer network.
- Build various models for attack mitigation.
- Validate with micro-grid test-bed and real datasets

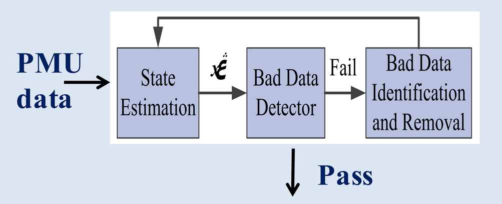


Scientific Impact:

- Anomaly detection and trust models for attack mitigation
- Situation-aware models for threat monitoring, analytics, decision control

Challenges: Inter-dependence, IoT Robustness, Cyber-Physical, Big Data

- Integrity mechanism for protection and state estimation



Broader Impacts:

- Influencing the standards
- Multi-disciplinary training in CPS security
- Experiential learning in real micro-grid facility.
- Outreach and research demo
- Generalization to other CPS

Missouri S&T Micro-grid

S. Tan, D. De, W. Song and S. K. Das, "Security Advances in Smart Grid: A Data Driven Approach," *IEEE Communications Surveys and Tutorials*, 2017.

Silent Perturbation of State Estimation

- Goal:
  - Damage power equipment
  - Increase system operation costs
  - Disproportionate power generation/dispatch or energy routing
  - Cause economic loss
- How?
  - Perturbing the state estimation
  - Fooling the system operator to make unnecessary and costly actions, such as generator rescheduling and load shedding.
- Assumptions:
  - IEC TR 61850-90-2 allows sending protection messages in plaintext.
  - Active adversary with MitM attack capability.
  - Adversarial knowledge:
    - *Known*: bad data detection threshold, i.e., # of states and measurements, topology of the power grid
    - *Unknown*: accurate knowledge of Jacobian measurement matrix.

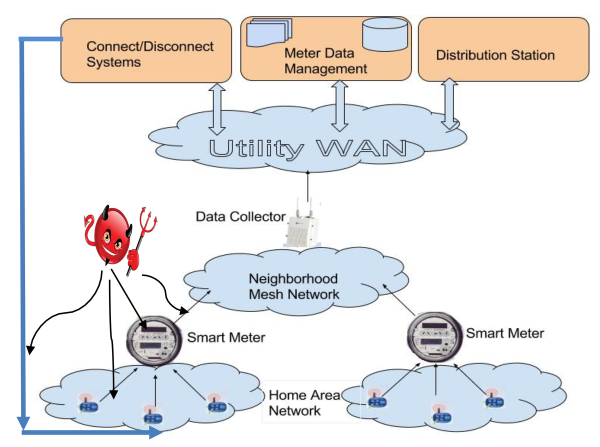
Smart Meter Data Falsification

Organized, Persistent Adversaries

- Circumvent cryptographic defense
- Compromise a large # of meters
- Attacks persist and evolve
- Mask easy consistency check
- Knowledge of business and revenue models

Challenges

- Consumption exhibits inherent fluctuations
- Distinguishing between legitimate and malicious changes
- Large no. of compromised nodes with smaller margin of false data
- Various falsification types



Attack Models

- *Additive*
- *Deductive*
- *Camouflage*
- *Conflict*
- Incremental Evolving, On-Off attacks, Omission, Order Aware Falsification Strategies

Proposed Trust Model

- Robust consensus formed through anomaly detection
- Use a Kullback-Leibler Divergence between historical and current proximity distributions of smart meter to the robust consensus R_t

$$X_i(t) = \begin{cases} 1 & \text{if } p_t^i(rep) \in \{\mu_t \pm \sigma_t\}; \\ 0 & \text{otherwise} \end{cases}$$ Historical Proximity

$$Y_i(t) = \begin{cases} 1 & \text{if } p_t^i(rep) \in \{\mu_{R_t} \pm \sigma_{R_t}\}; \\ 0 & \text{otherwise} \end{cases}$$ Current Proximity

$X_i(t)$ → probability parameter r

$Y_i(t)$ → probability parameter q

$$D_i(X_i \| Y_i) = (1-r) \times \ln\left(\frac{1-r}{1-q}\right) + p \times \ln\left(\frac{r}{q}\right)$$ → Kernel Methods

Integrity of Protection Messages

- Challenges
  - Most recent mp in substations use ARM Cortex-M cores
    - Cannot meet 4ms requirement for hash based integrity checking or encryption
  - Need a very light weight but secure mechanism.
- Our Approach
  - Permutation only encryption
- Algorithm
  - Generate 16-bit Fletcher checksum
  - Generate a set of random numbers based on a seed
  - Sort the numbers & use them as offsets for checksum bits
  - Hide checksum bits in the message
- Key management
  - Initially communicated to all receivers securely.
  - Salted with status and renegotiated when counter rolls over.

- Security Analysis
  - 96 bit security
  - Key salting ensures security against known/chosen plaintext attacks
  - Success probability before the key changes is negligible.
  - Secure from off-path attacks
- Performance Analysis
  - Real implementation on a 48 MHz ARM cortex mp

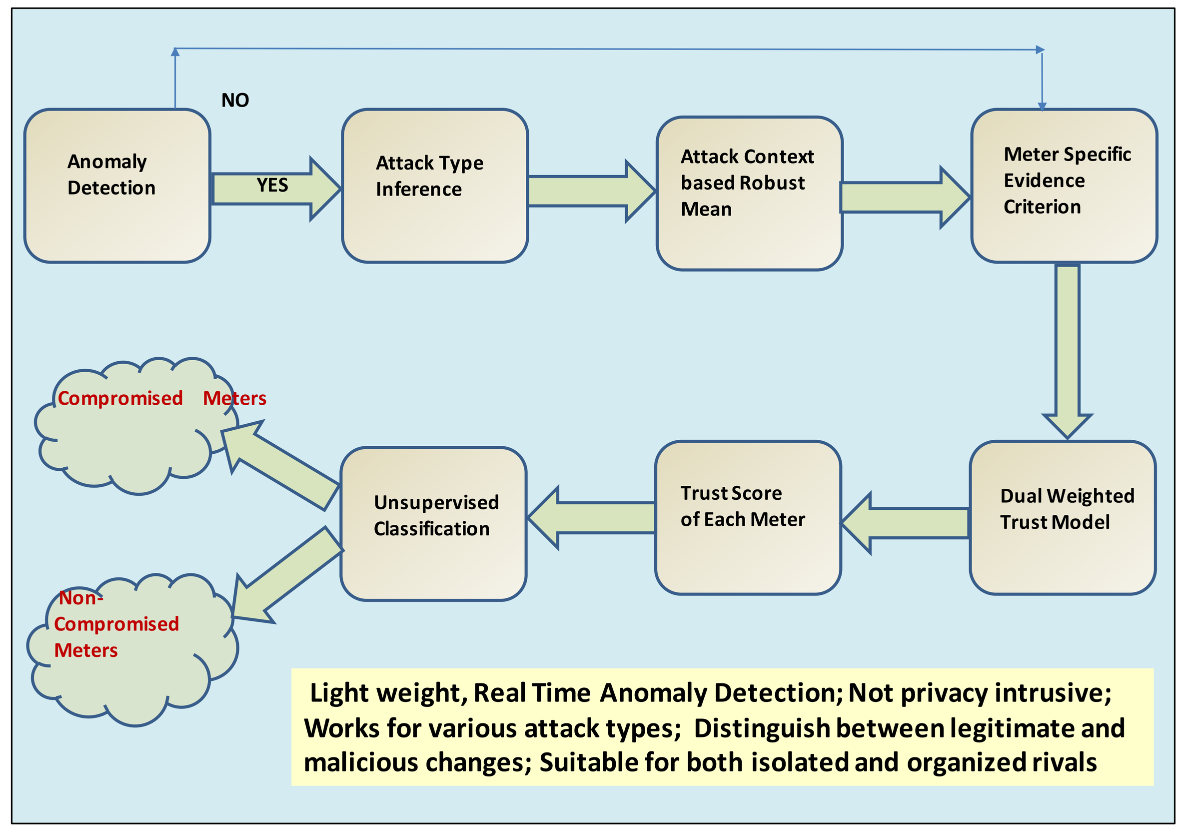
Algorithm	Speed (KB/s)
Proposed Method	424
MD5	147
ChaCha20-Poly1305	94
AES-128-CCM	70
AES-128-EAX	70
AES-128-GCM	41

- Publication: Kant, K. and Jolfaei, A. 2017. A Lightweight Integrity Protection Scheme for Fast Communications in Smart Grid, 14th International Conference on Security and Cryptography (SECRYPT), Jul. 24–26, Madrid, Spain, pp. 31-42.

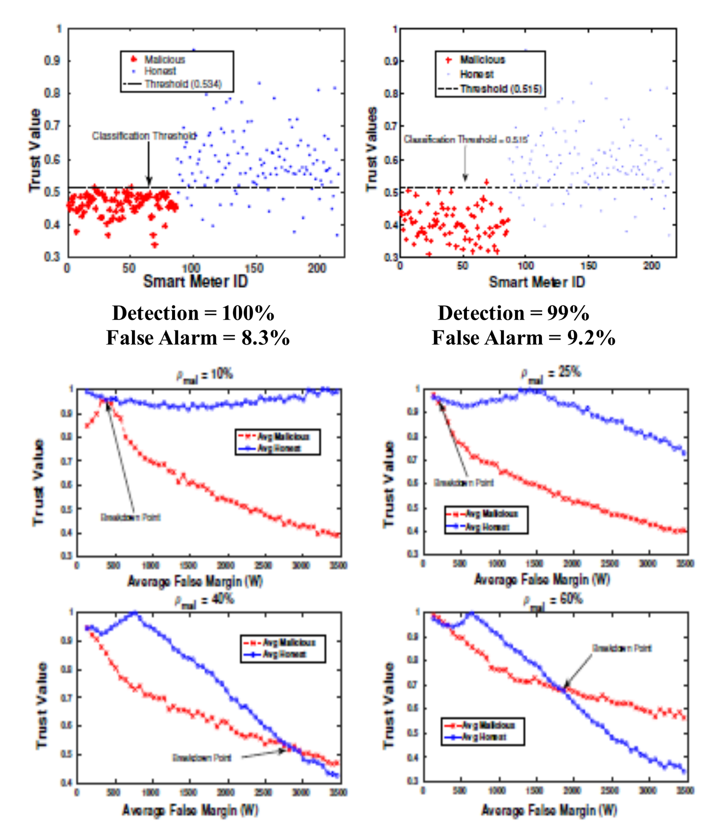
Attack Procedure

- Bypass bad data detection
  - Malicious measurements pass the bad measurement detection if the *L2* norm of the attack vector ≤ the bad data detection threshold.
- Adversary reconstructs the entries of measurement Jacobian matrix within the maximum error margin of a small percentage.
  - Small perturbations in the measurements can lead to a large drift in the state value if the smallest singular value of the Jacobian measurement matrix is small.
- It is theoretically/practically impossible to spoof a large number of measurements at once.
  - States are perturbed partially/gradually in different rounds of state estimation.
- Drift state values within a desired range
  - Linear unidirectional changes in voltage magnitudes and phase angles.
  - Impulsive and/or oscillatory modifications.
  - The acceptable range of voltage amplitude variation is within ±5%.

Proposed Framework: Overview



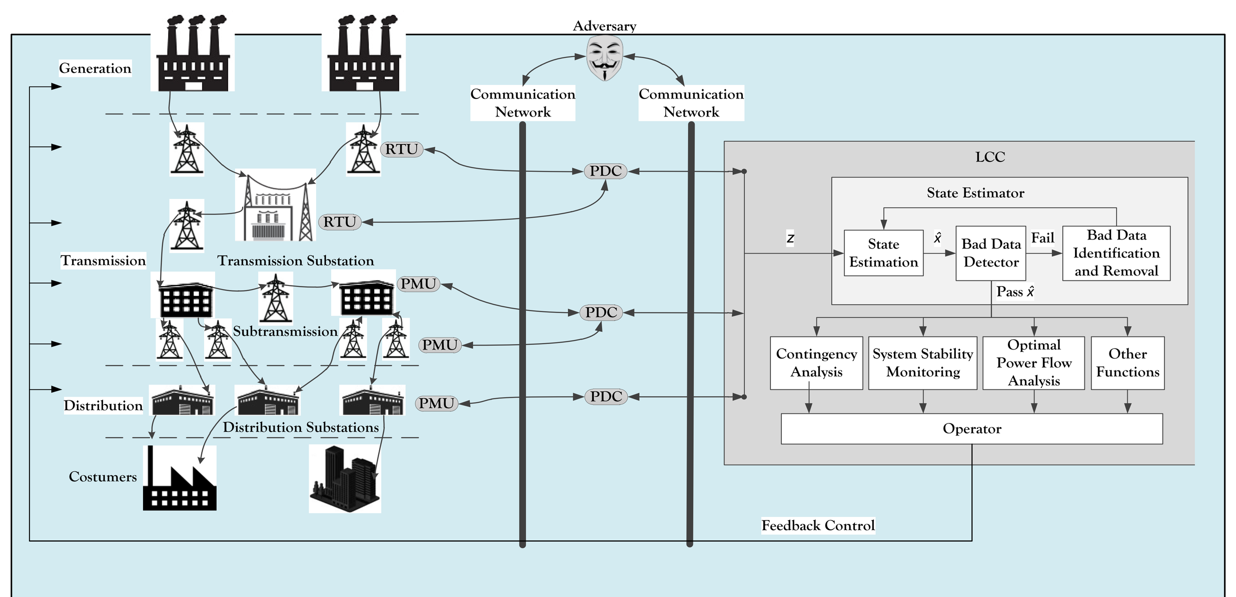
Performance Evaluation



- We use real data set from PECAN Street Project (SmartGridGov) and Irish Data Sets.
- We emulate attacks on real data fed to a virtual simulated AMI
- We observe clears difference between compromised and non-compromised nodes.
- Results[1] are better due the robustness of statistical measures used in various steps

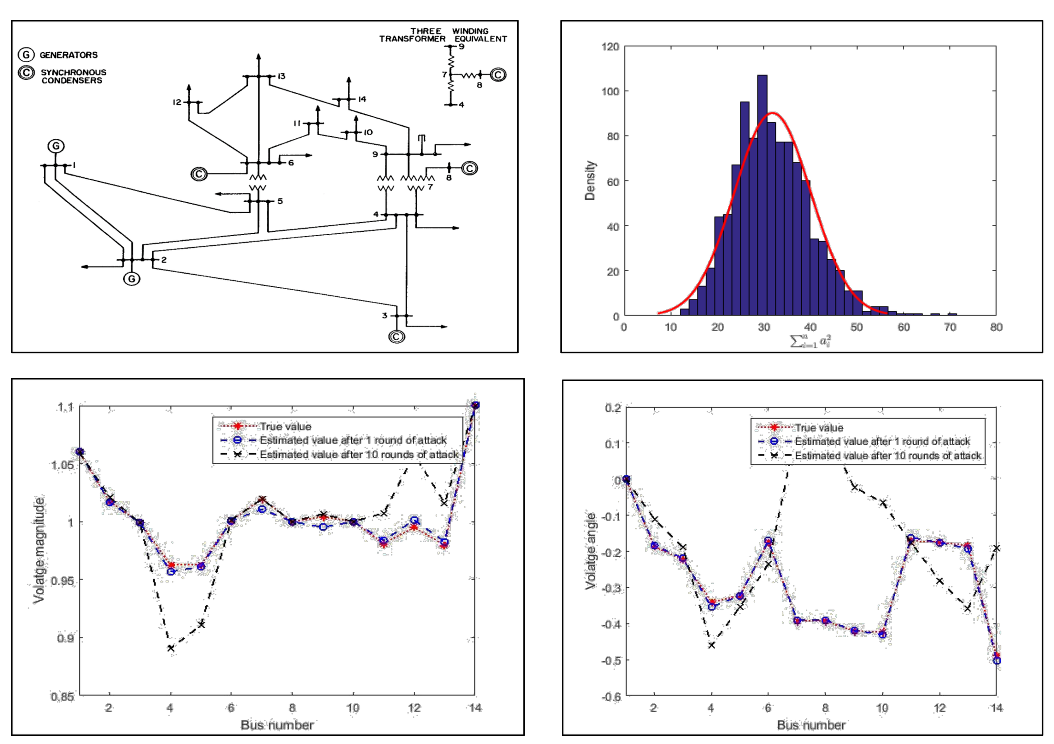
Bhattacharjee, Thakur, Silvestri, Das, et.al. "Statistical Security Incident Forensics against Data Falsification in Smart Grid Advanced Metering Infrastructure," *ACM CODASPY, 2017.*

Smart Grid Management

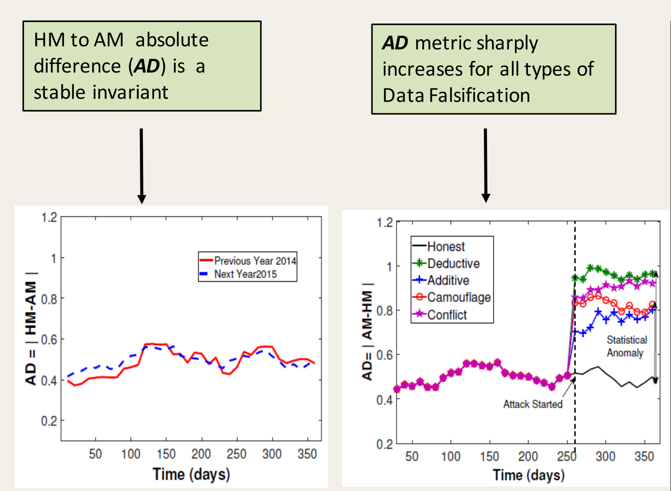


- Kant, K. and Jolfaei, A. 2017. On the Silent Perturbation of State Estimation in Smart Grid, IEEE Journal of Selected Topics in Signal Processing, Under Review.

Evaluation



Proposed Anomaly Detection



AD	AM	HM	GM	Conclusion
Increased	Increased	Increased	Increased	Additive
Increased	Decreased	Decreased	Decreased	Deductive
Increased	Same	Decreased	Decreased	Camouflage
Increased	Any	Any	Any	Conflict
Same	Don't Care	Don't Care	Don't Care	No Attack

- A rise in the absolute difference of HM and AM is a reliable indication of occurrence of organized falsification
- Anomaly detection metric is stable without any smoothening average technique
- The property holds for all different datasets studied. e.g. Texas, Ireland datasets

Ongoing Research

- Stealthy and Persistent Attacks
  - Advanced Information Theoretic Approaches beyond divergence measures
  - State-less (short term) and State-full (long term) Detectors.
  - Decrease the false alarm rates without sacrificing detection rate.
  - Margins of false data below 400, Unsupervised and scalable.
- Robust state estimation
  - Silent state perturbation mechanisms with partial knowledge of network parameters
  - Mitigation mechanisms
- PMU data falsification
  - Identify compromised meters
  - Formalize supervised and unsupervised learning techniques