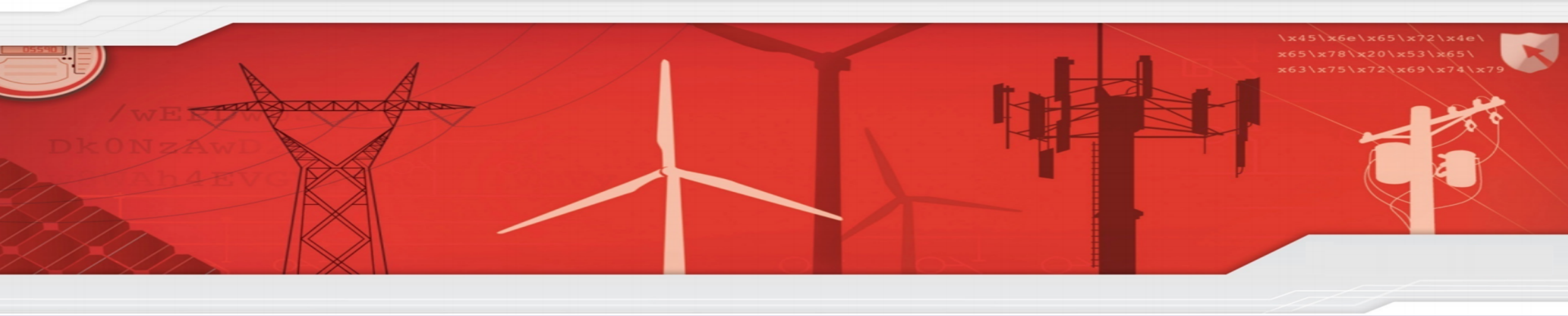


CPS: Breakthrough:

Securing Smart Grid by Understanding Communications Infrastructure Dependencies

(Sept 1, 2015 – Aug 31, 2018)

CNS-1544904
Krishna Kant
Arvind Srinivasan
Temple University

CNS-1545037
Sajal K. Das
Simone Silvestri
Mariesa Crow
Missouri Univ. of Science & Technology

Overview and Goals

Objectives

- Ensuring integrity and robustness of Smart Grid (SG) communications.
- Detecting and mitigating attacks and failures.

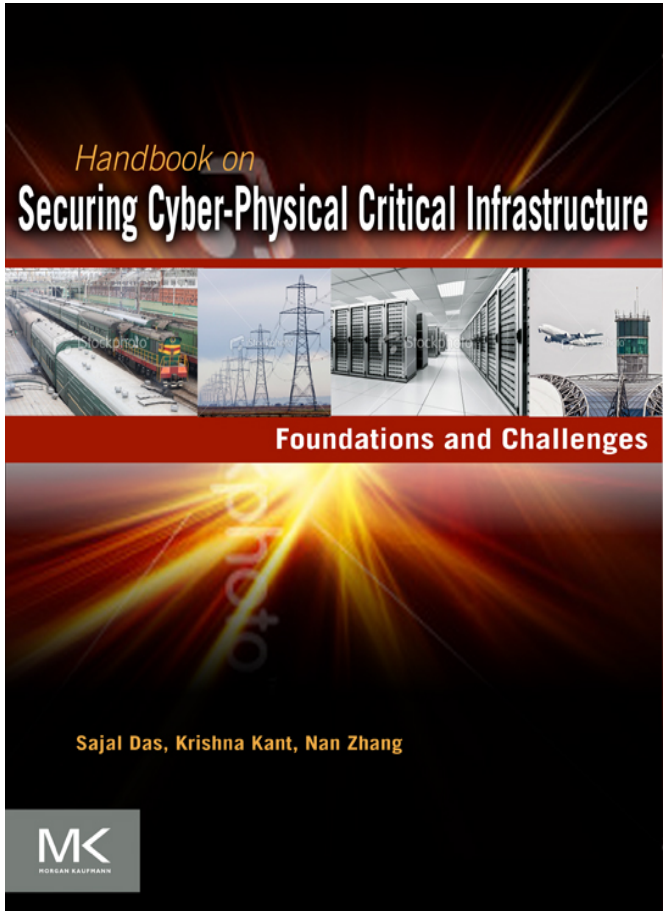
Challenges: Interdependency, Robustness, Cyber-Physical, Big Data

Specific Tasks

- Characterize dependence between SG and communication systems.
- Make SG communication protocol and state estimation more robust.
- Build models for compromised node and attack detection.
- Mitigate propagation of impacts of attacks and cascaded failures.
- Validate models with experimentation on a micro-grid test-bed.

Thrust I

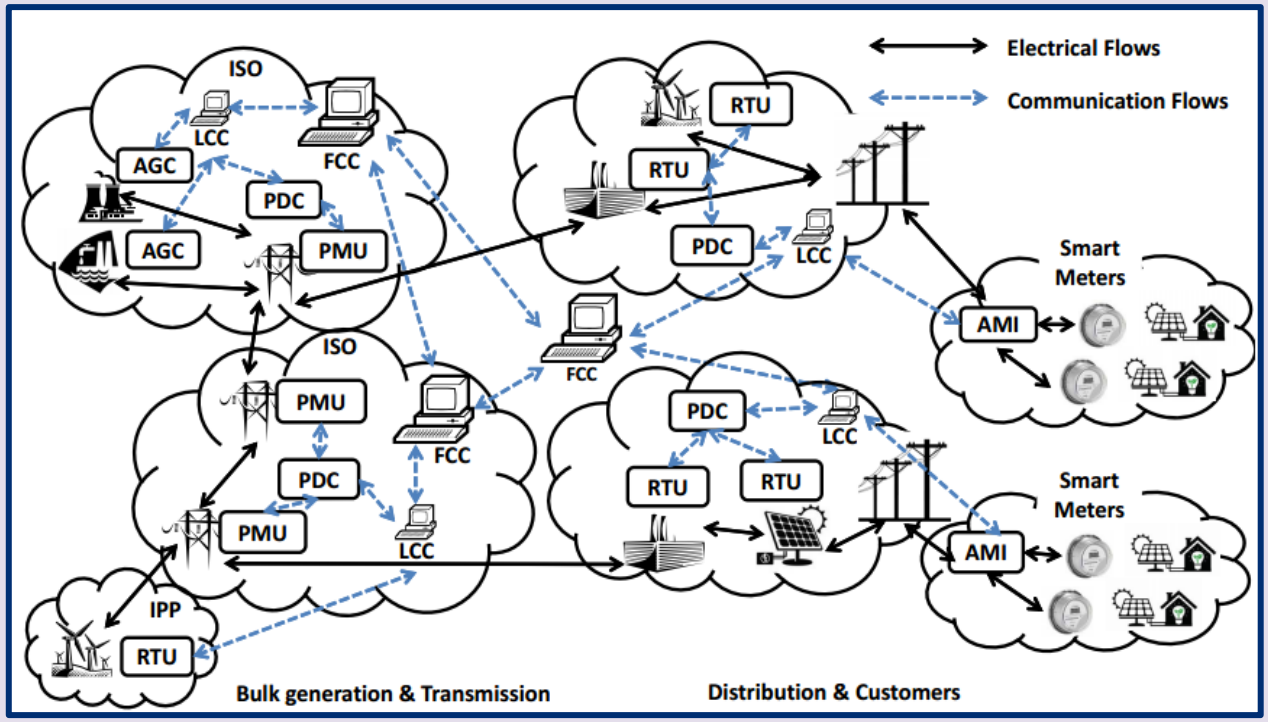
- Making Smart Grid communication protocols and state estimation more robust
  - Designing low latency integrity mechanism
  - Silent state perturbation and its mitigation



Smart Grid (SG) Structure

Applications

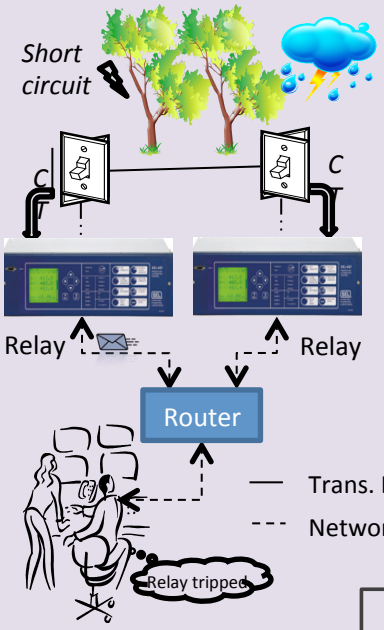
- Power flow monitoring
- Power conditioning
- Protection
- Degradation monitoring



Comm. Standards

- IEC 61850 (2004):
  - Standard for substation automation function; includes a standard communication protocol.
- IEEE C37.118 (2005), updated 2011
  - Synchrophasor measurement & test specs, PMU data formats
- IEC TR 61850-90-5 (2012):
  - Data exchange between PMUs, PDCs, Wide Area Monitoring, Protection, and Control (WAMPAC), and control center applications.

Smart Grid Management



Energy Management System

State perturbation in small undetectable steps

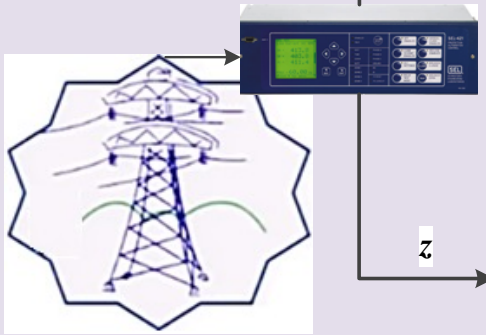
State Estimator

State Estimation → $x\hat{\alpha}$ → Bad Data Detector → Fail → Bad Data Identification and Removal

Pass $x\hat{\alpha}$

- Short Circuit Calculation
- Contingency Analysis
- Optimal Power Flow Analysis
- Model Validation
- Frequency and Voltage Stability Monitoring

z

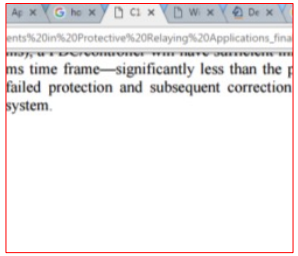


z

Power System Protection

(4ms Tight Latency)

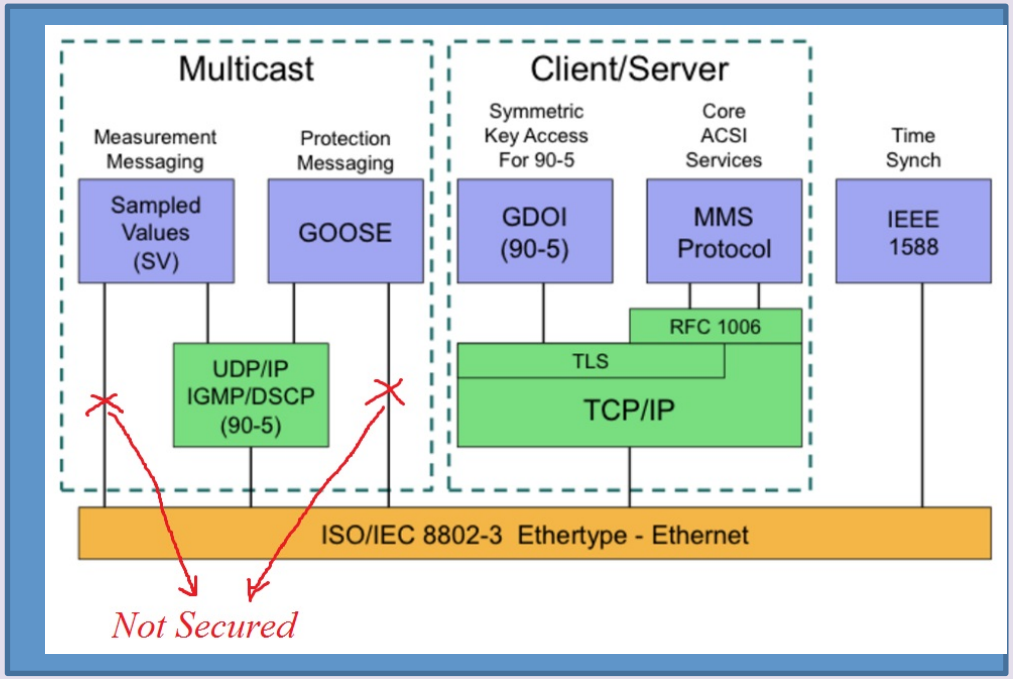
Integrity violation due to lack of security



- Short Circuit Calculation
- Relay Protection
- Oscillation Detection
- Frequency and Voltage Stability Monitoring

Communications & Security in IEC61850

- Several integrity schemes, indicated by an enumerated value.
  - Value 0: Intended for protection. Low latency ➔ No encryption/HMAC.
  - Others: May not be implemented in practice



Modules in green defined in 2012 standard, currently not deployed

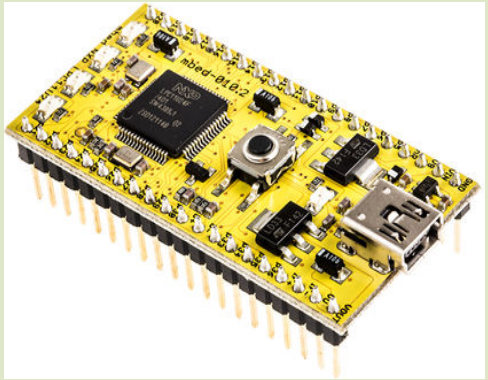
Allowed values for MAC (msg auth code) signature value calculations

Enum value	HMAC algorithm	No. of bits	Designation
0	None	None	MAC-None
1	SHA-256	80	HMAC-SHA256-80
2	SHA-256	128	HMAC-SHA256-128
3	SHA-256	256	HMAC-SHA256-256
4	AES-GMAC	64	AES-GMAC-64
5	AES-GMAC	128	AES-GMAC-128

Integrity of Protection Messages

Challenges

- Most recent μP in substations use ARM Cortex-M cores
  - Cannot meet 4ms requirement for hash based integrity checking or encryption
- Injection/corruption of protection message can cause havoc
- Need a very light weight but secure mechanism



Embedded LPC11U24 at 48 MHz frequency

Our Approach

- Permutation only encryption

Basic Algorithm

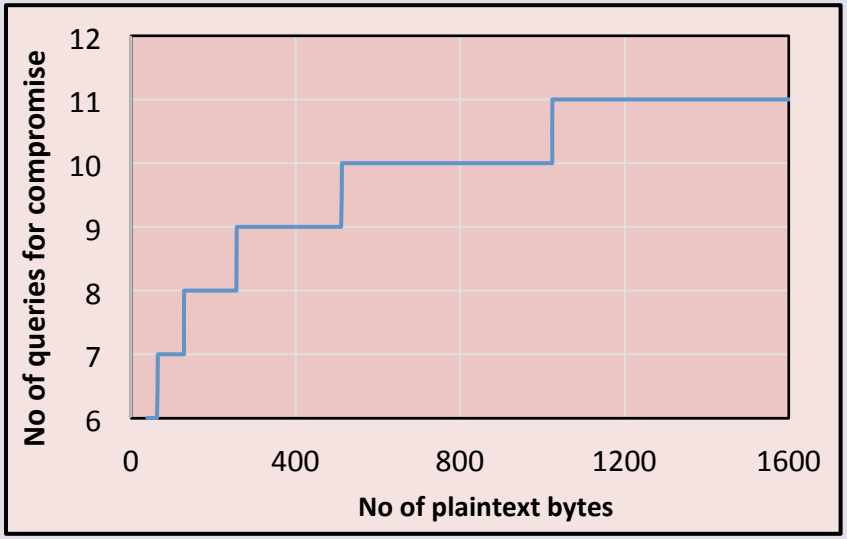
- Generate 16-bit Fletcher checksum
- Generate a set of random numbers based on a seed (= Key)
- Sort the numbers & use them as offsets for checksum bits
- Hide checksum bits in the message

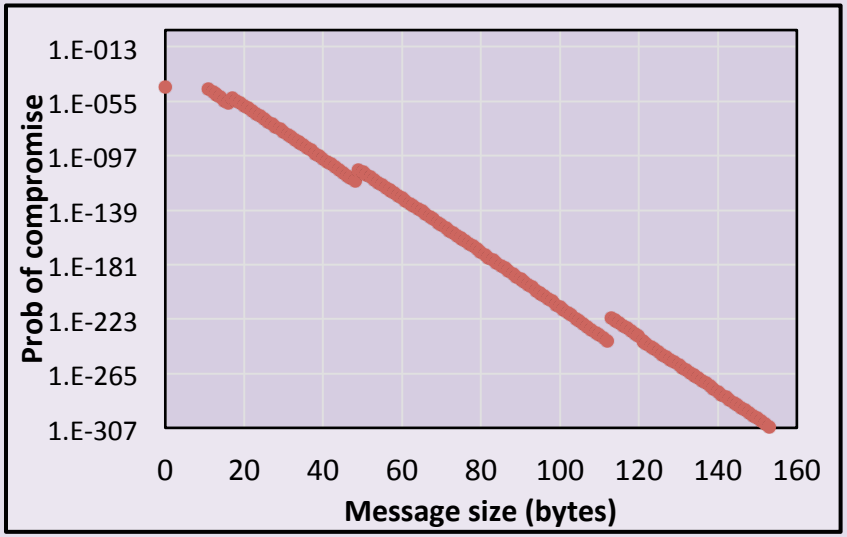
Key management

- Initially communicated to all receivers securely.
- Salted with status number (a 32-bit counter) every $\lceil \log_2(8N + 16) \rceil - 1$ transmissions
  - N = Min number of plaintext bytes
- Key renegotiated when counter rolls over.

Security Analysis

- Brute-force attacks: 96 bit security
- Ciphertext-only attacks
  - Checksum recalculation is more cumbersome than brute-forcing.
- Known/chosen plaintext attacks
  - Key salting ensures security
- Related key attacks
  - Secure from off-path attacks
  - Key disclosed from permutation indices.
    - Success probability before the key changes is negligible.



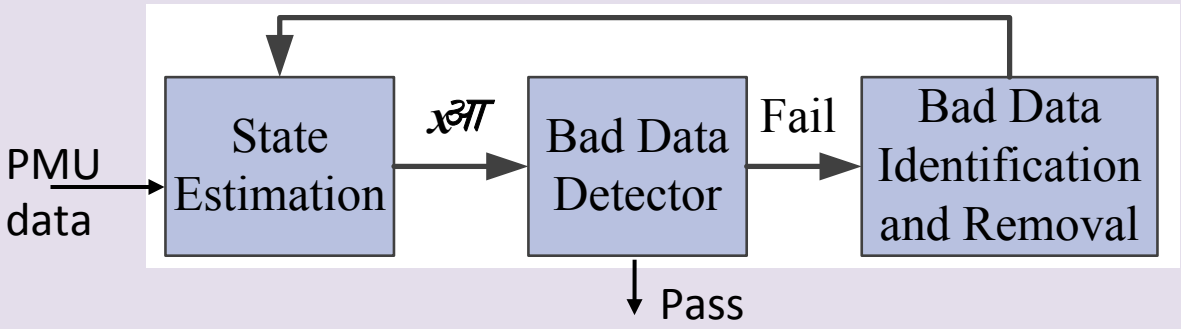


Performance Analysis

- Real implementation on a 48 MHz ARM cortex μP
- Comparison against other high speed approaches
- Results
  - ✓ Fastest – about 3x of next best algorithm
  - ✓ Only one that can satisfy the requirement of 4 ms.
  - ✓ Actual latency of 2.5 ms
  - ✓ Useful in other applications also.

Algorithm	Speed (kilobytes per second)
Proposed method	424
MD5	147
ChaCha20-Poly1305	94
AES-128-CCM	70
AES-128-EAX	70
AES-128-GCM	41

Silent State Perturbation

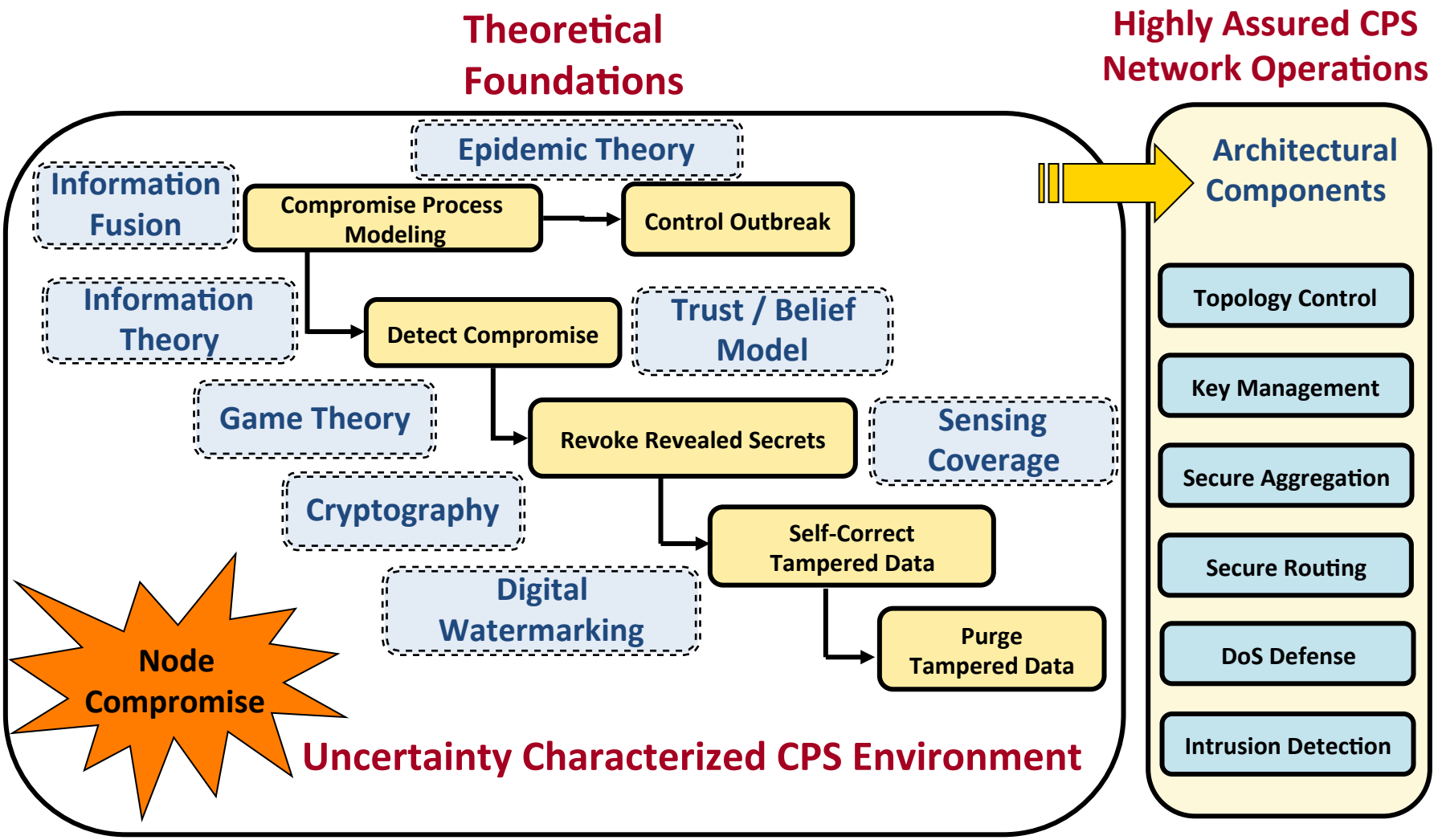


- Attack
  - Perturb measurements w/o triggering bad data detection
  - Repeat attack to silently amplify perturbation
    - Only some state variables can be perturbed; choose ones that maximize grid disturbance
- Mechanisms
  - Prior work assuming Jacobian matrix (H) is fully known
  - New mechanisms based on partial knowledge of H matrix
- Attack mitigation
  - Countermeasures against silent perturbation attacks

Thrust II

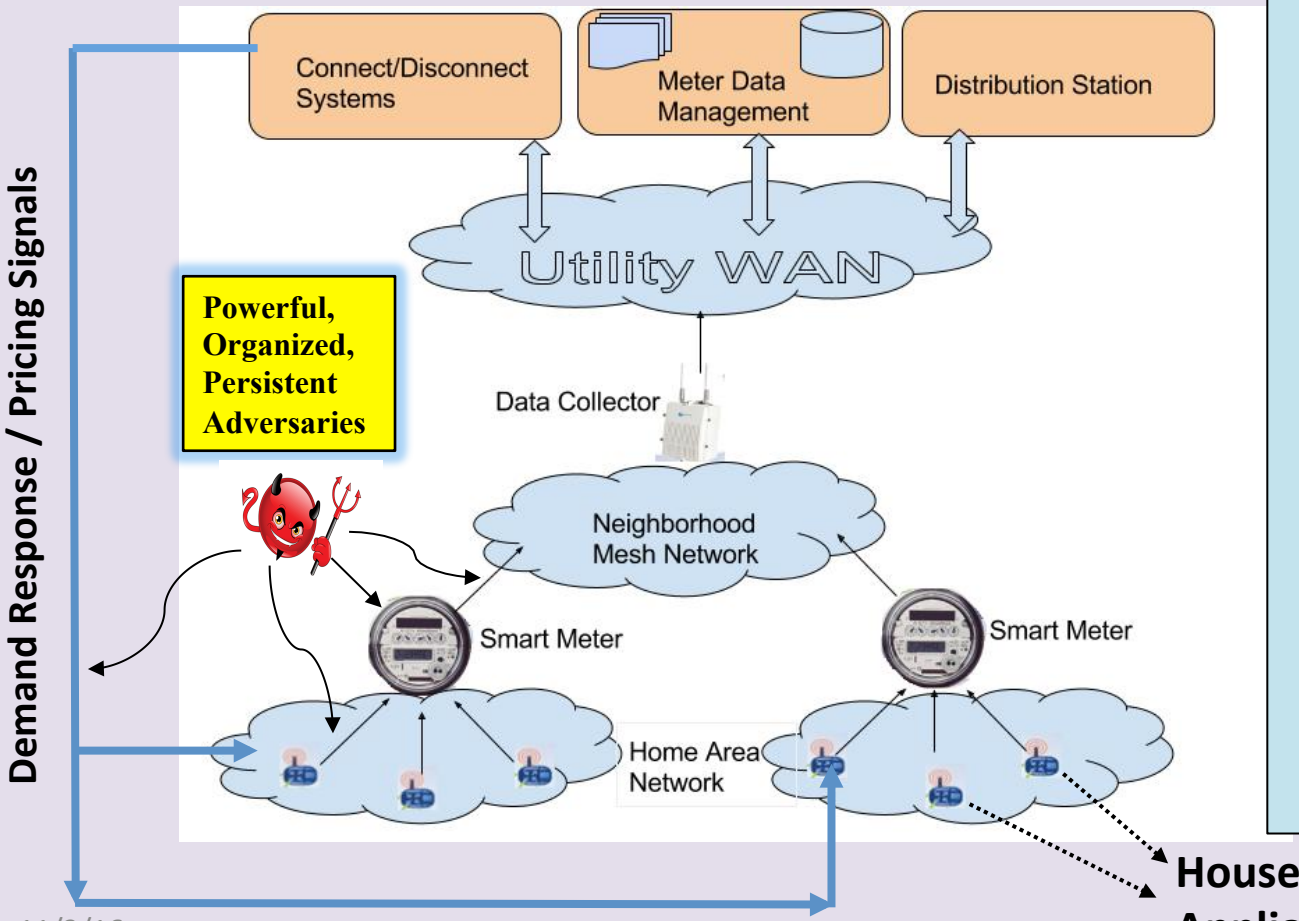
- Attack detection and mitigation in advanced metering infrastructure (AMI)
  - Attack models and node compromises
  - False data injection
  - Trust model

Multi-Level CPS Security Framework



Advanced Metering Infrastructure (AMI) Micro-Grid

- **Functions of AMI**
  - Automated Billing
  - Demand Response (DR)



- **Securing the Smart Grid**
  - Integrity violation of smart metering data in transit
  - State perturbation and false data injection
  - AMI attacks
  - Billing system vulnerabilities
  - Power system side attacks

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

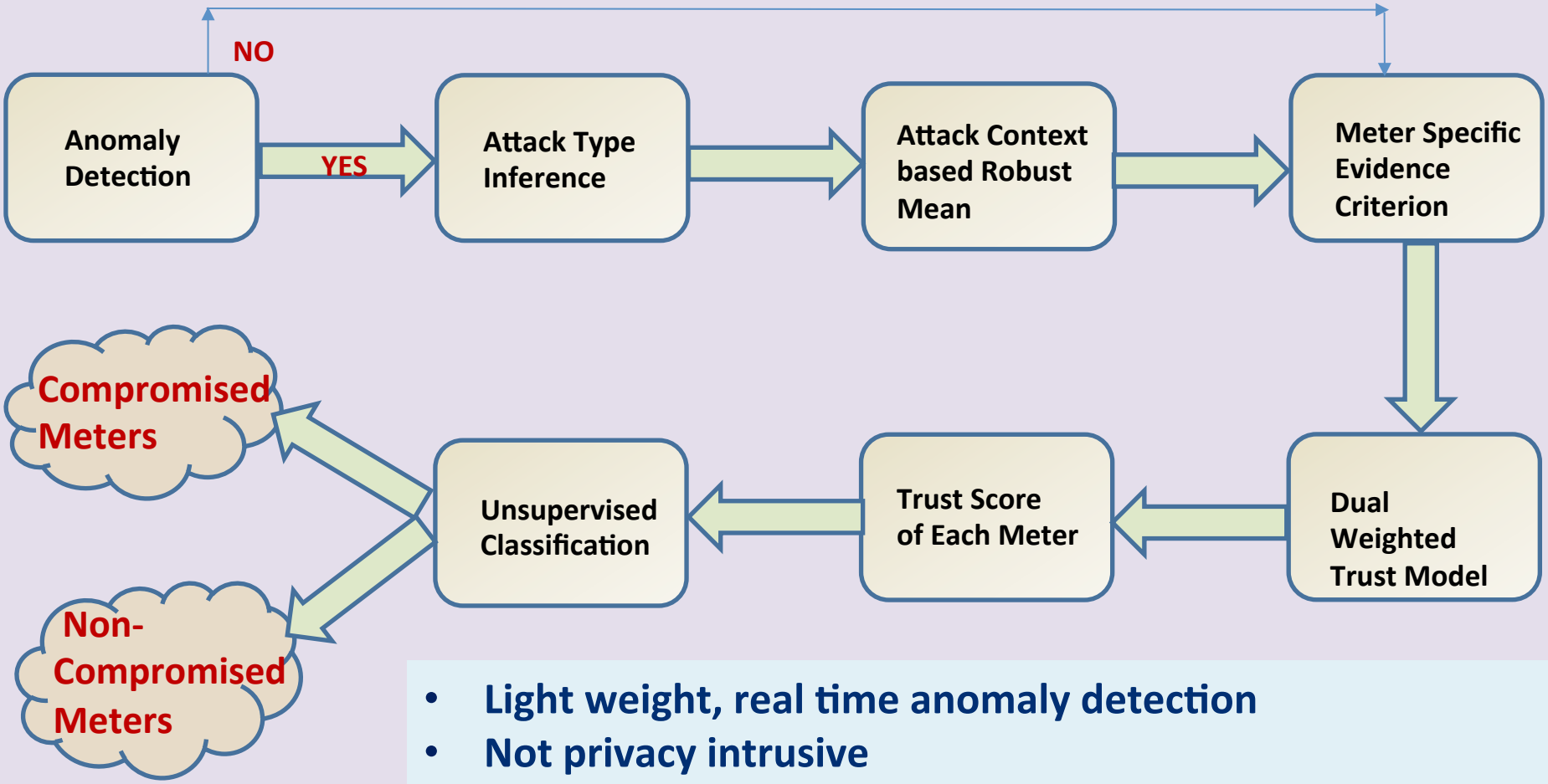
Challenges:

- Consumption exhibits inherent fluctuations
- Distinguishing between legitimate and malicious changes
- Large # of Compromised Nodes with Smaller Margin of False Data
- Various Falsification Types

Attack Models:

- **Additive:** Reports greater than actual power consumption
- **Deductive:** Reports lesser than actual power consumption
- **Camouflage**: Balance additive & deductive attacks from different meters
- **Conflict**: Unbalanced additive and deductive attacks from multiple uncoordinated adversaries

Proposed Approach



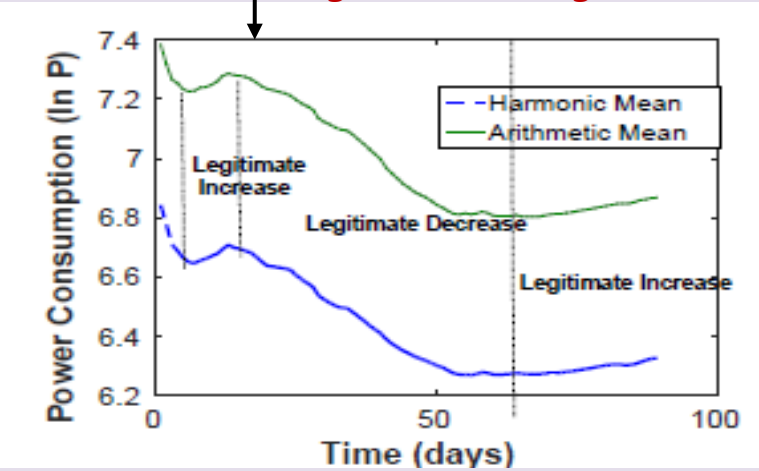
- Light weight, real time anomaly detection
- Not privacy intrusive
- Works for various attack types
- Distinguishes between legitimate and malicious changes
- Suitable for both isolated and organized attacks

Legitimate and Malicious Changes

- Transform the observed data into a Gaussian mixture
- A light weight statistical indicator for anomalies: Ratio of Harmonic Mean (HM) to Arithmetic Mean (AM) of the Gaussian

HM and AM of mixture data change due to legitimate weather and other contextual factors

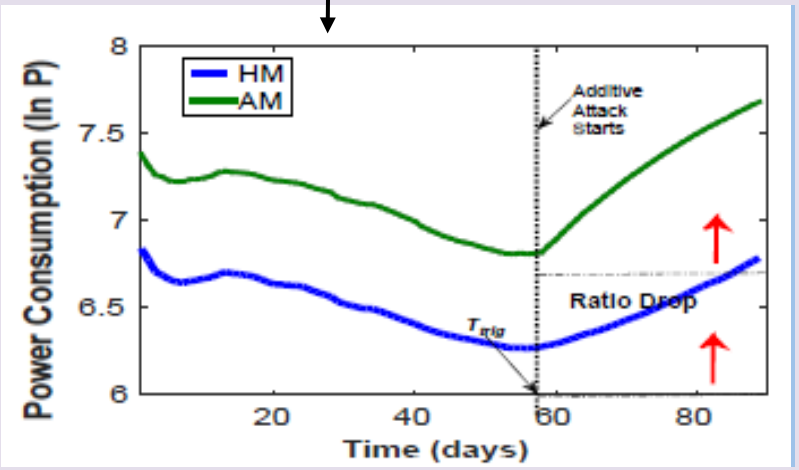
Symmetric Change in HM and AM under legitimate change



HM vs. AM: Legitimate Data

HM and AM may change due to data falsification

Asymmetric Change in HM and AM under attacks

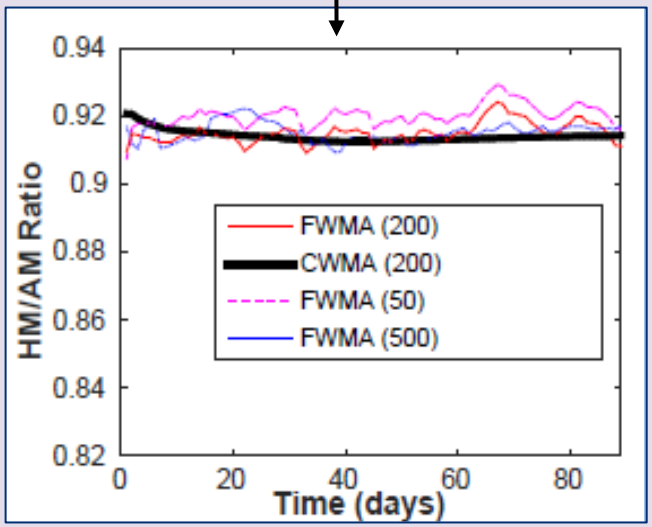


HM vs. AM: Under Attacks

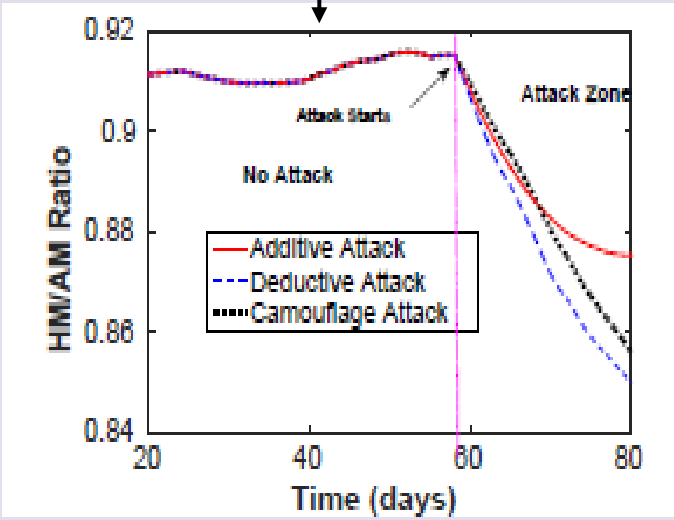
Intuition: *Track ratio of HM to AM*

Anomaly Detection

HM to AM ratio highly stable against legitimate changes

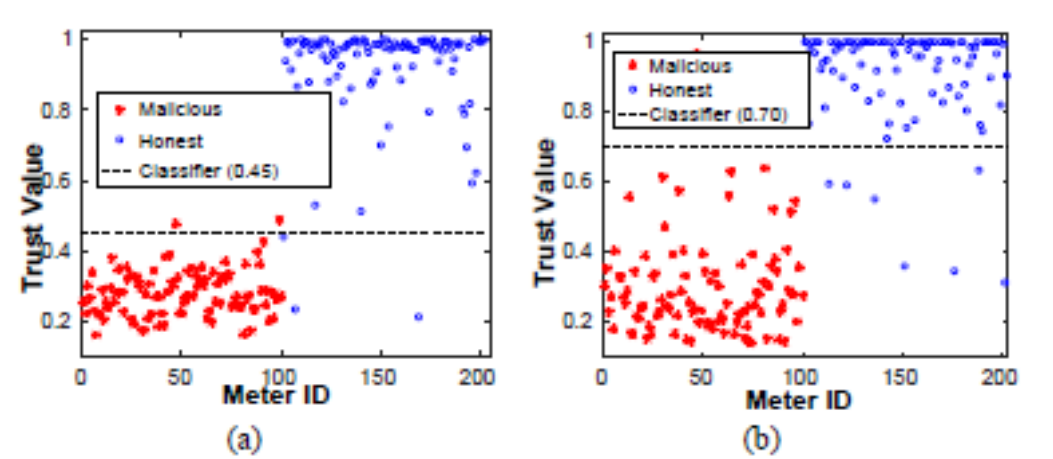


HM to AM ratio drops for all types of Data Falsification

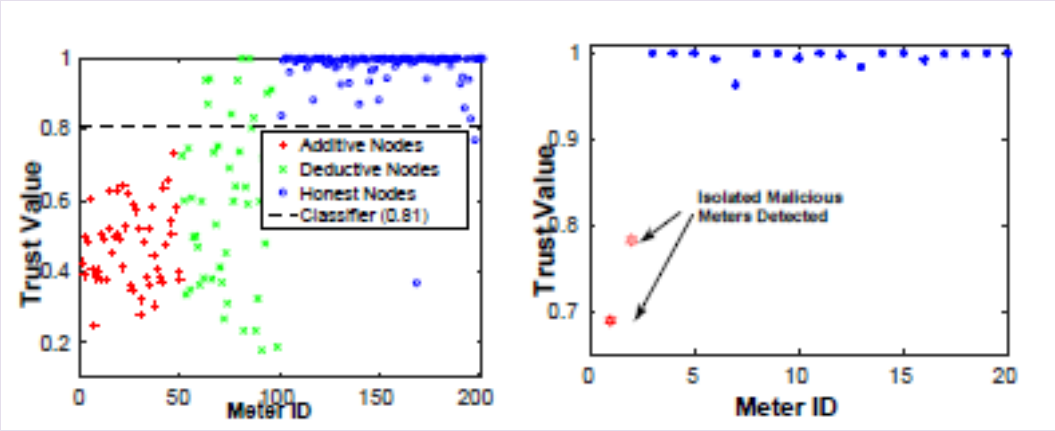


- A drop in HM to AM ratio is an indication of organized falsification
- The ratio is maintained as forgetting and cumulative moving averages
- Property holds for all attack types and higher fraction of compromised nodes

Performance Evaluation



Avg. Trust Values (a) Additive (b) Deductive



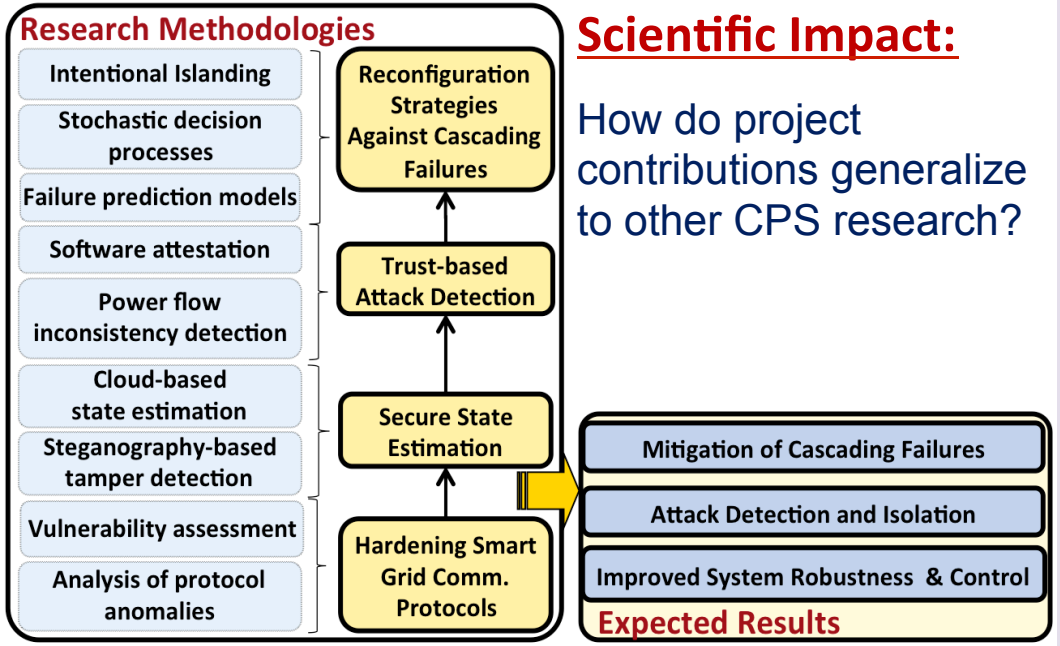
Avg. Trust Values (a) Camouflage (b) Isolated Attacks

- Used real data set from PECAN Street Project (SmartGridGov)
- Emulated attacks on real data fed to a virtual simulated AMI
- Observed clear difference between compromised & non-compromised nodes
- Results are better due to robustness of statistical measures in various steps
- Works for isolated attacks

Summary

Objectives:

- Characterize interdependence between Smart Grid & comm systems
- Make protocols & state estimation more robust
- Detect impacts (failures and attacks) and prevent cascades.
- Build models for attack mitigation.
- Validate with real test-bed.



Scientific Impact:

How do project contributions generalize to other CPS research?

Solution Methodologies:

- Integrity mechanism for protection & state estimation
- IEC81650 Protocol hardening
- Game theory and trust models for attack detection, failure spreading
- Situation-aware models for threat monitoring, analytics, decision control

Broader Impacts:

- Influencing the standards.
- Multi-disciplinary security training in CPS.
- Experiential learning in real-life micro-grid facility.
- Outreach, demo and research showcase

Micro-grid at Missouri S&T

Ongoing Research

- **Integrity protection**
  - Key management protocols
- **Robust state estimation**
  - Silent state perturbation mechanisms with partial knowledge of network parameters
  - Mitigation mechanisms
- **Vulnerability analysis of GOOSE protocol and hardening**
- **PMU data falsification**
  - Identify compromised meters
  - Formalize supervised and unsupervised learning techniques
- **Cascade failures**
  - Electrical Topology based prediction of time to cascade failures
  - Topology aware hardening of components against failure or attacks