Securing Smart Grid by Understanding Communications Infrastructure Dependencies

SAJAL DAS, MISSOURI UNIVERSITY OF SCIENCE & TECHNOLOGY

Cybersecurity Research Acceleration Workshop and Showcase, Indianapolis, IN
October 11, 2017

MISSOURI UNIVERSITY OF SCIENCE AND TECHNOLOGY
Formerly University of Missouri-Rolla

MISSOURI S&T

Computer Science Department

NSF CPS - Breakthrough:

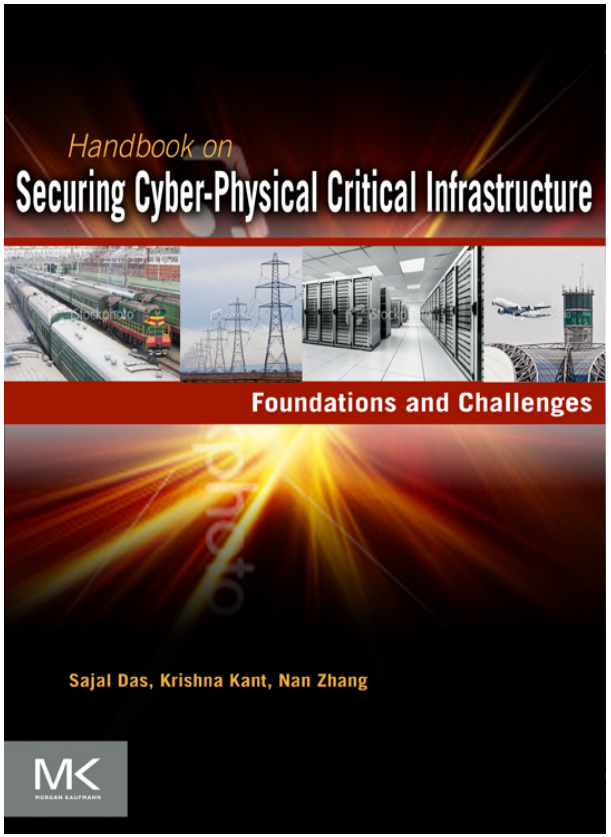
Securing Smart Grid by Understanding Communications Infrastructure Dependencies

Sajal K. Das

sdas@mst.edu

(Bhattacharjee, Thakur, Silvestri, Das,

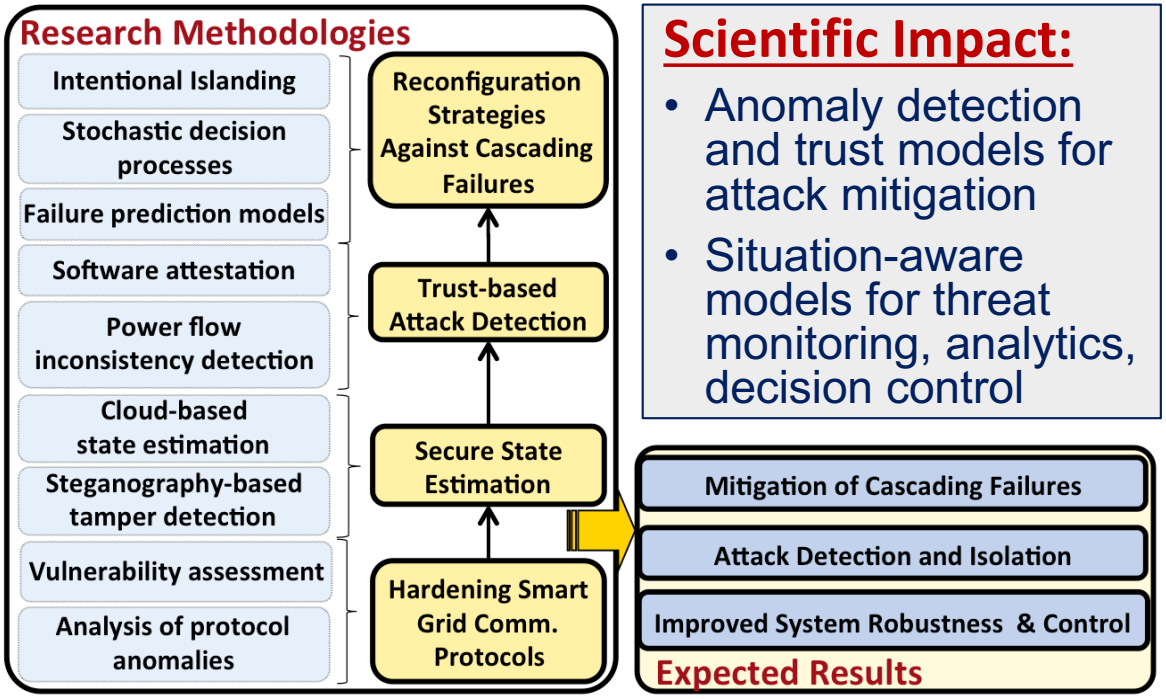
ACM CODASPY 2017)



NSF CPS - Breakthrough: Securing Smart Grid by Understanding Communications Infrastructure Dependencies (PI: Sajal K. Das)

Objectives:

- Characterize inter-dependence between electrical grid and communication systems
- Make Smart Grid protocols and state estimation more robust
- Detect impacts (failures and attacks) and prevent cascades
- Build models for attack mitigation
- Validate with micro-grid test-bed

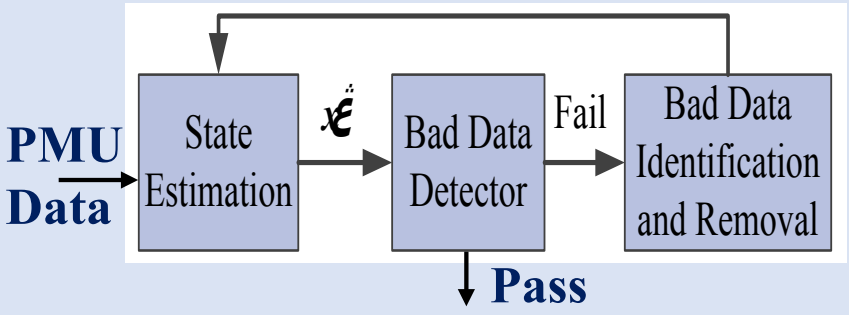


Scientific Impact:

- 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



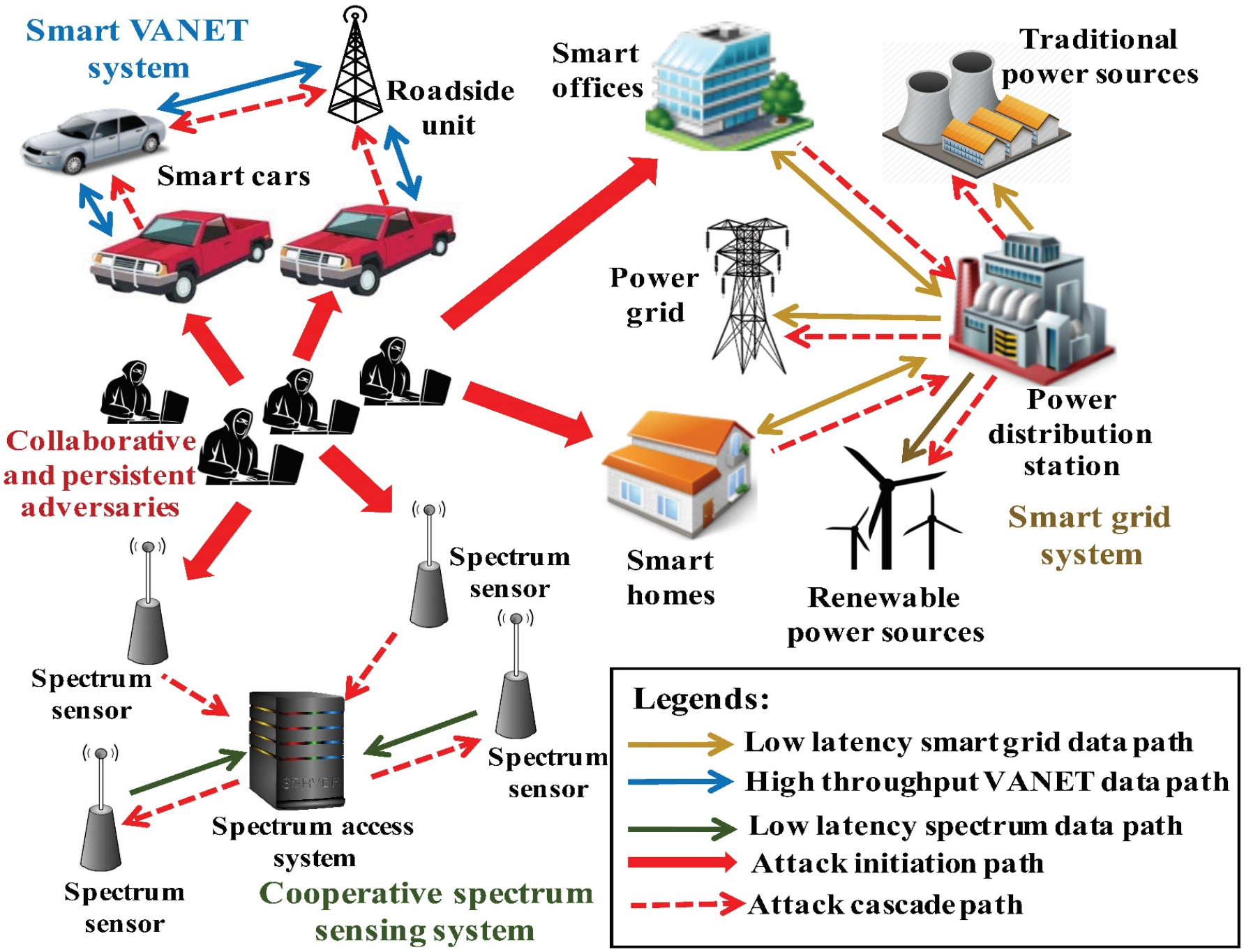
Broader Impacts:

- 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.

Example IoT Systems: Smart City Scenario



IoT Enables Cyber-Physical Systems (CPS)

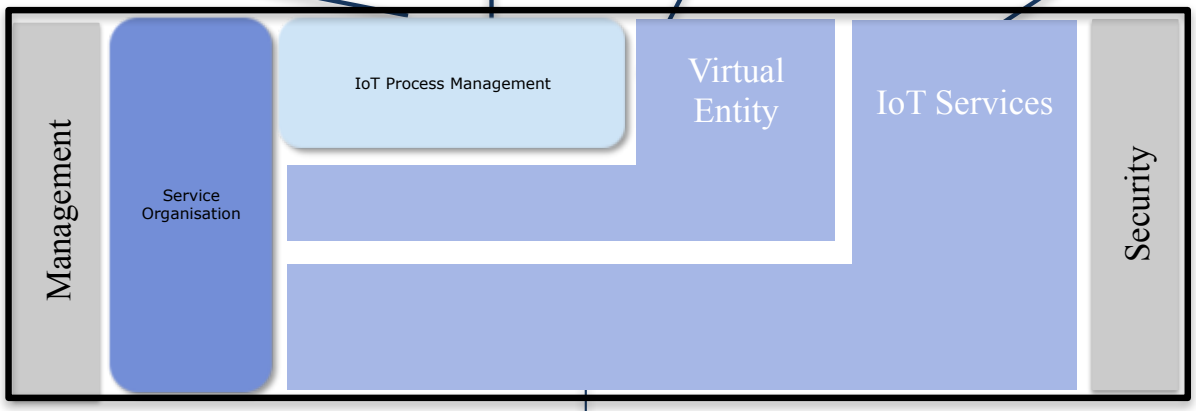
Smart Energy Management

Smart Healthcare

Smart Transportation

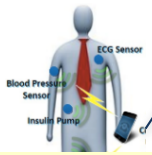
Smart Water Management

IoT Middleware



Sensor/Actuator Networks

Body Area Networks



SensorCloud

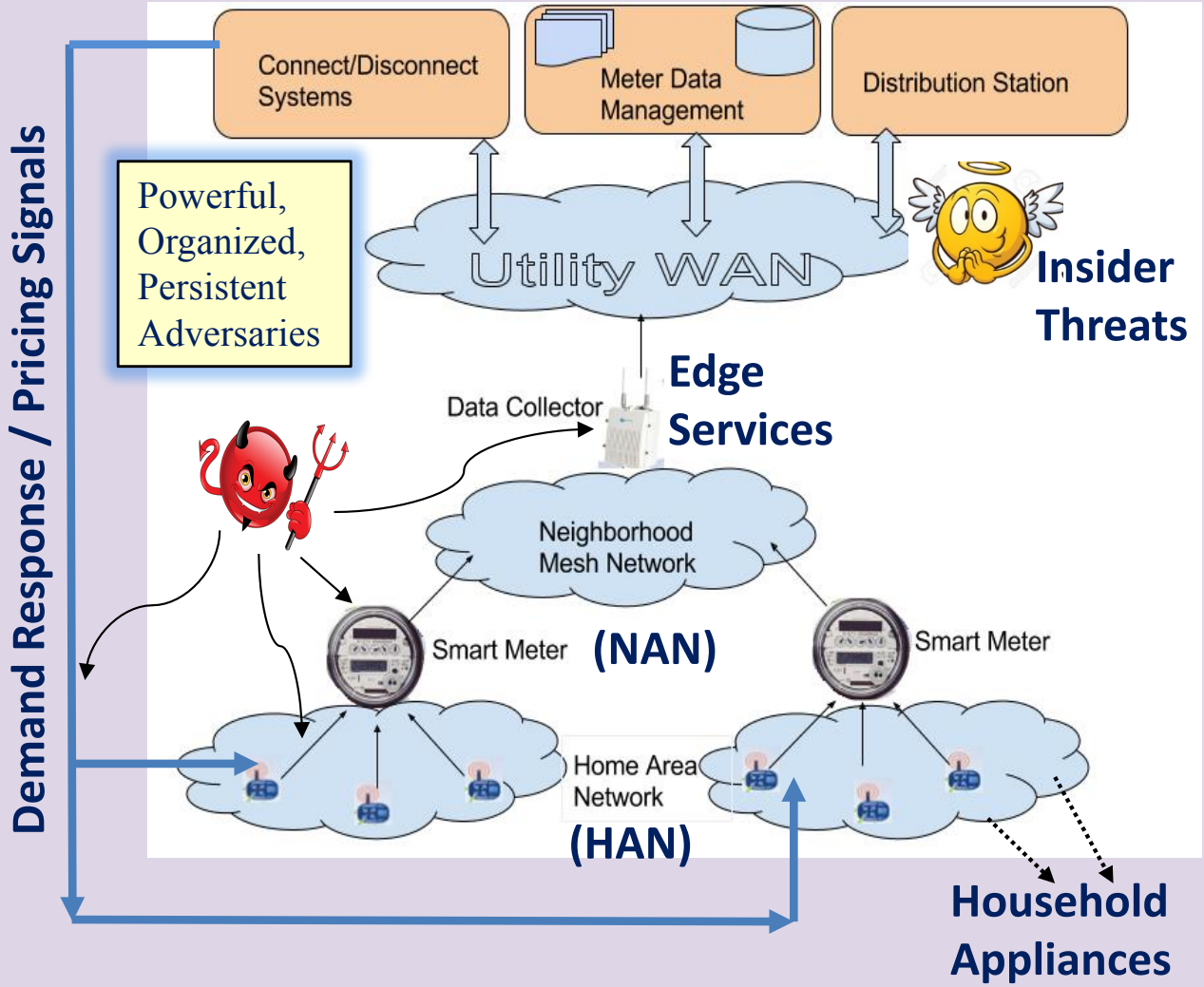
Characteristics: Complex System of Systems, Large-scale, Heterogeneous, IoT, Big Data

Challenges: **Inter-dependence, Robustness, Safety, Security, Reliability, Resiliency**

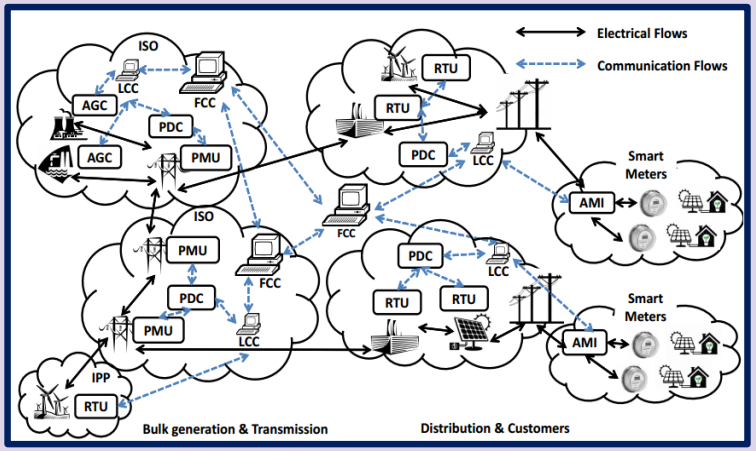
Advanced Metering Infrastructure (AMI) Micro-Grid

Functions of AMI

- Automated Billing
- Demand Response (DR)



Smart Grid Architecture



Securing Smart Grid

- Integrity violation of smart metering data in transit
- State perturbation and false data injection
- AMI attack detection and mitigation
- Attack and trust models
- Billing system vulnerability

IoT and CPS Security – Who Cares?

We all care … because our lives are at stake …

Smart electricity meters can be dangerously insecure (Mar 2017) – Hackers can cause fraud, explosions and house fires.

Hackers could turn your smart meter into a bomb and blow your family to smithereens

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

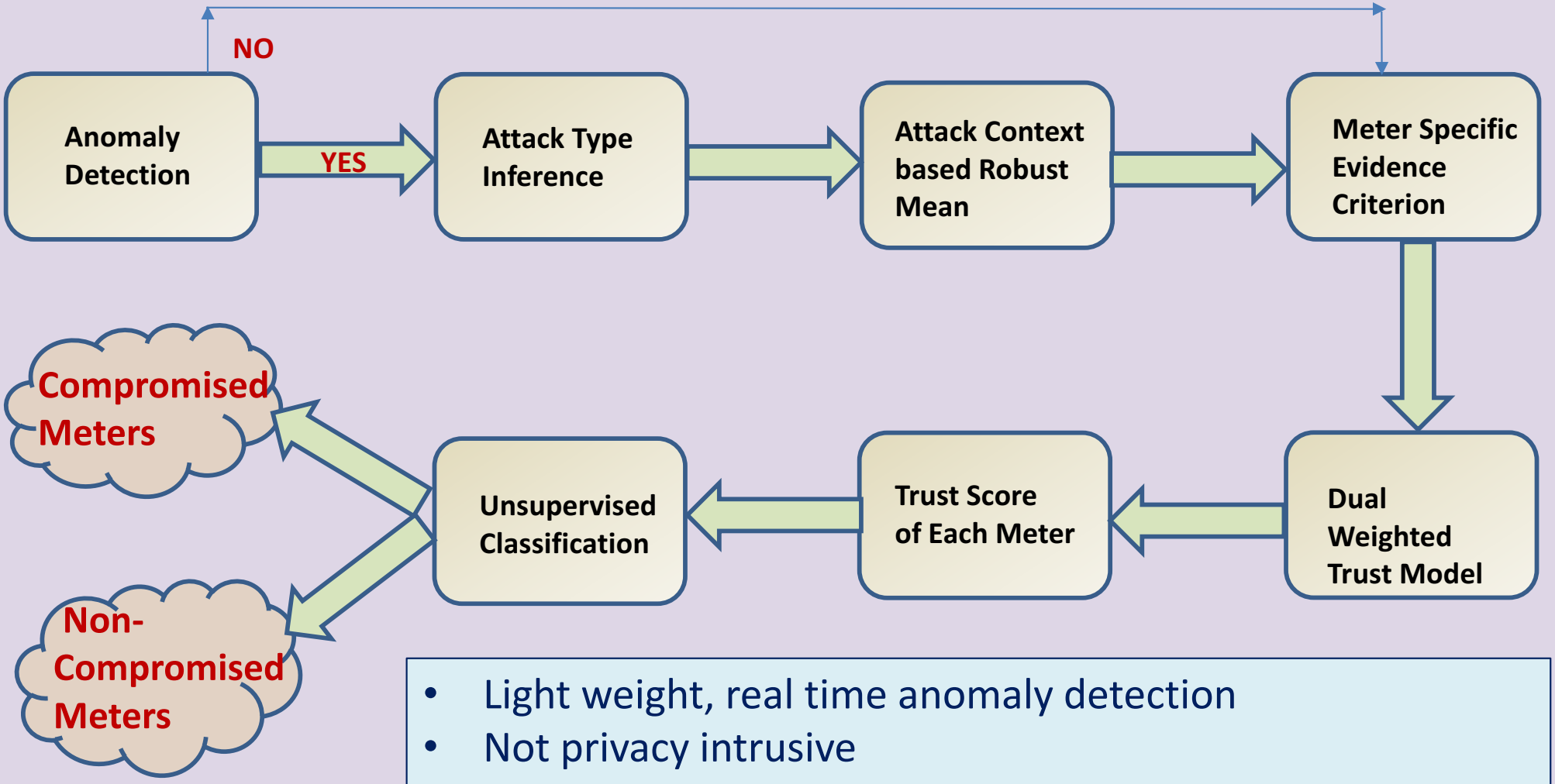
Challenges:

- 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



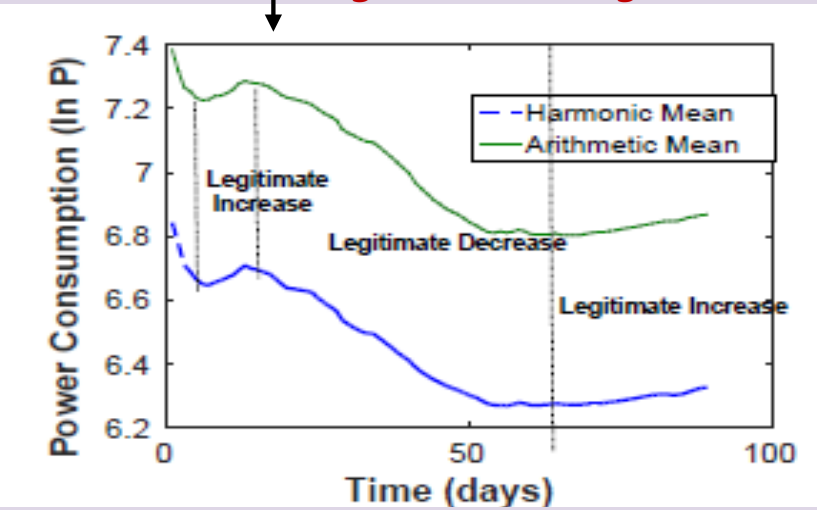
- Light weight, real time anomaly detection
- Not privacy intrusive
- Works for various attack types
- Distinguishes between legitimate and malicious changes
- Suitable for both isolated and organized attacks

Legitimate and Malicious Changes

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

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

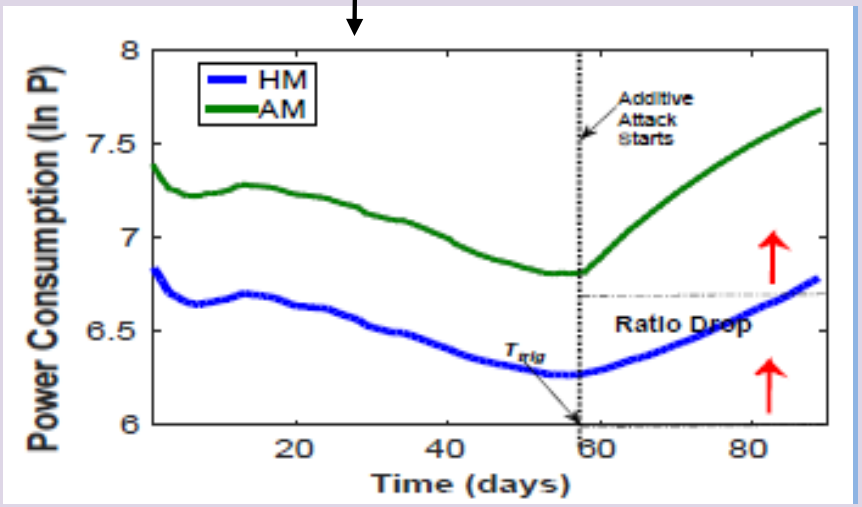
Symmetric Change in HM and AM under legitimate change



HM vs. AM: Legitimate Data

HM and AM may change due to data falsification

Asymmetric Change in HM and AM under attacks

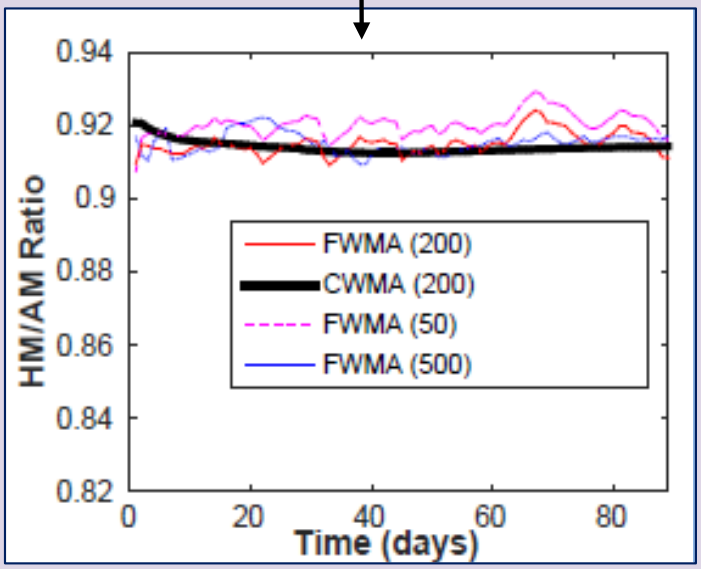


HM vs. AM: Under Attacks

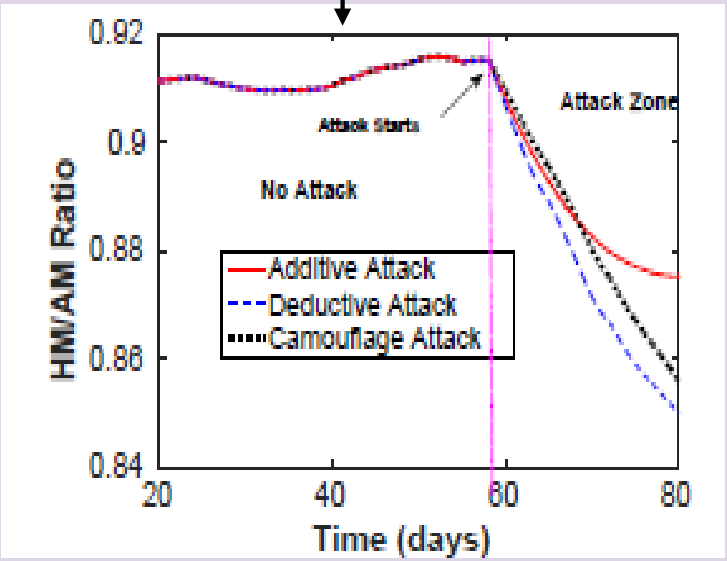
Intuition: ***Track HM to AM Ratio***

Anomaly Detection

HM to AM ratio highly stable against legitimate changes

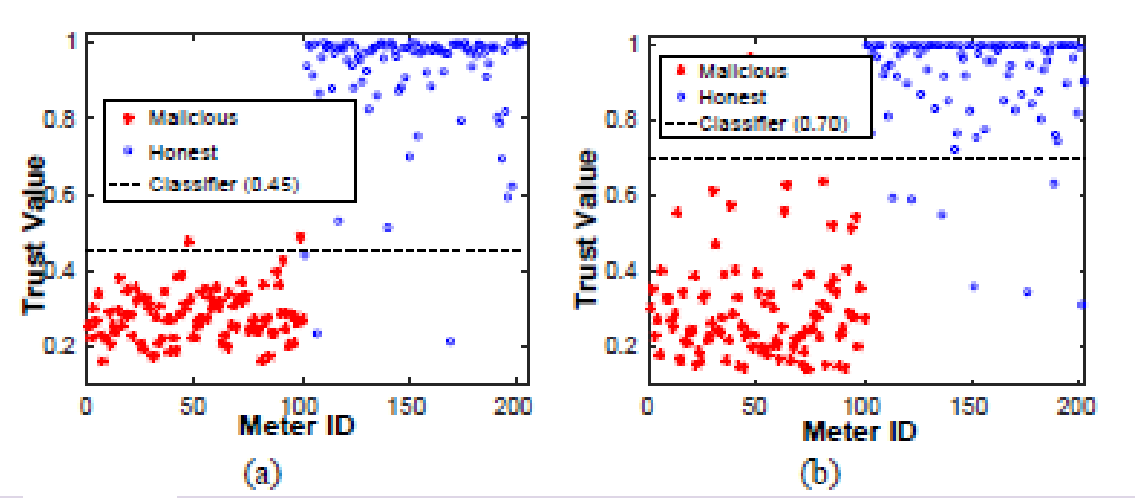


HM to AM ratio drops for all types of Data Falsification

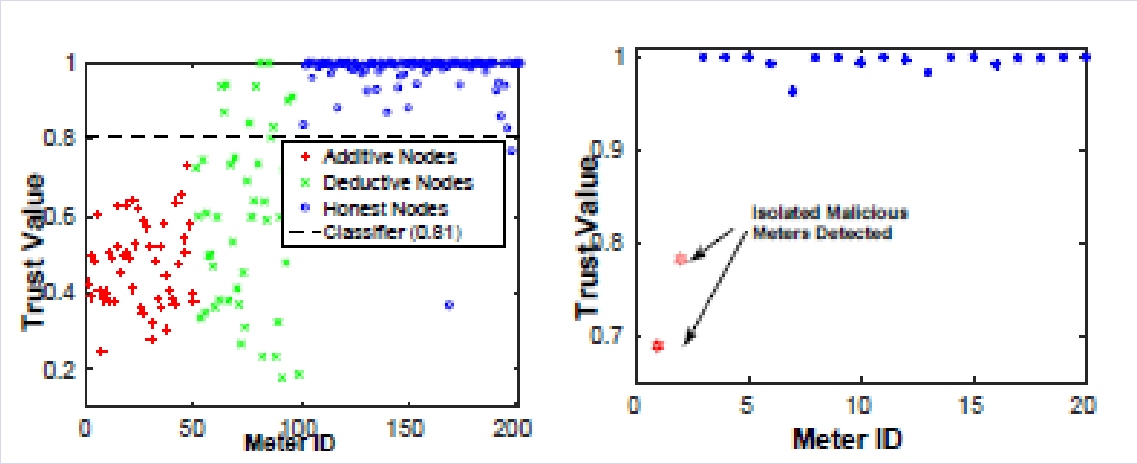


- A drop in HM to AM ratio is an indication of organized falsification
- The ratio is maintained as forgetting and cumulative moving averages
- Property holds for all attack types and higher fraction of compromised nodes

Performance Evaluation



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



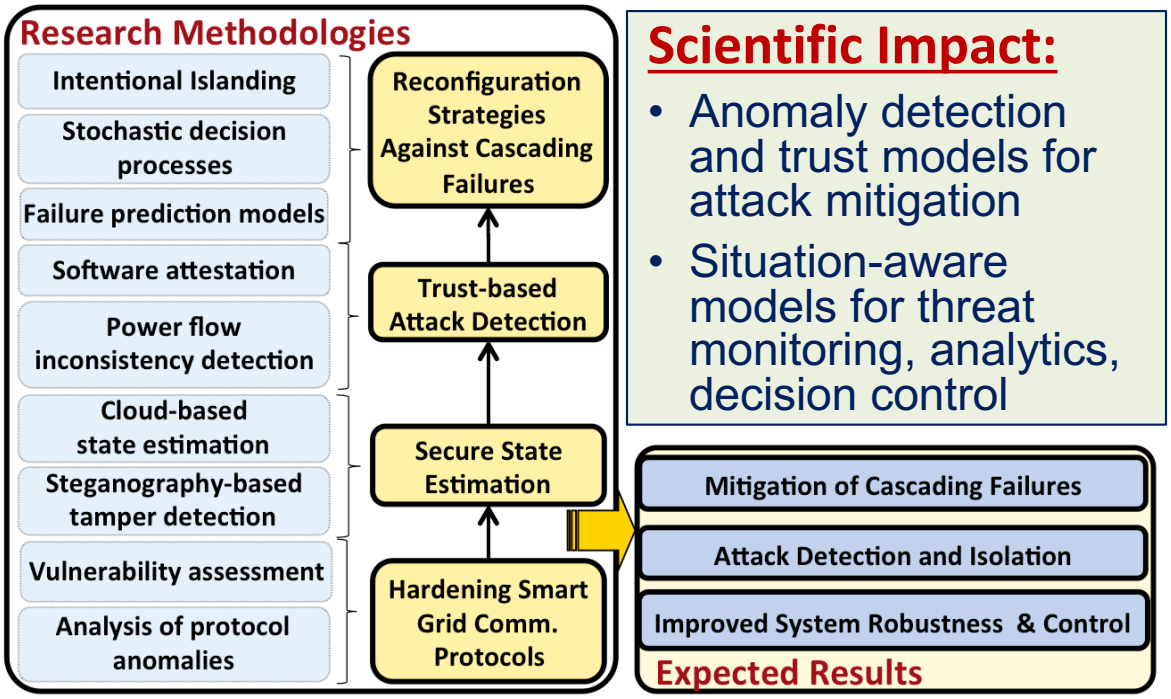
Avg. Trust Values (a) Camouflage (b) Isolated Attacks

- Used real data set from PECAN Street Project in Texas (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

NSF CPS - Breakthrough: Securing Smart Grid by Understanding Communications Infrastructure Dependencies (PI: Sajal K. Das)

Objectives:

- Characterize inter-dependence between electrical grid and communication systems
- Make Smart Grid protocols and state estimation more robust
- Detect impacts (failures and attacks) and prevent cascades
- Build models for attack mitigation
- Validate with micro-grid test-bed

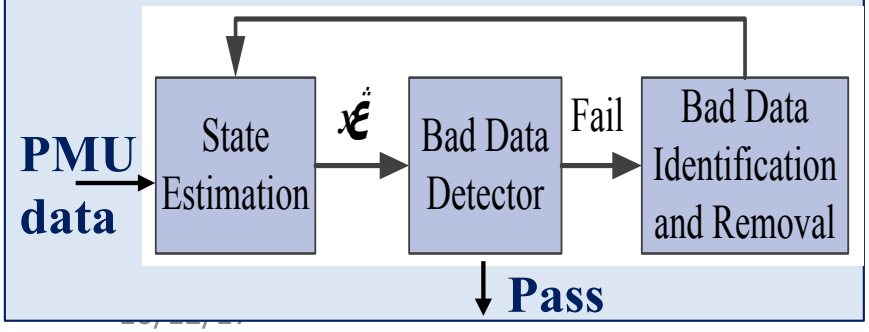


Scientific Impact:

- 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-rid

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.