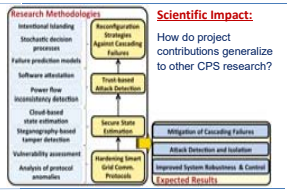
Collaborative Proposal: Securing Smart Grid by Understanding Communications Infrastructure Dependencies

CNS-1544904 (Lead: K. Kant, Temple University)
CNS-1545037 (Lead: Sajal K. Das, Missouri S&T)

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

Microgrid at Missouri S&T

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
  - Injection/corruption of protection message can cause havoc
  - Need a very light weight but secure mechanism

Embed 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 $\lceil \log2(8N + 16) \rceil - 1$ transmissions
    - N = Min number of plaintext bytes
  - Key renegotiated when counter rolls over.

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

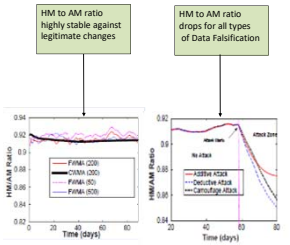
Challenges:

- 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:

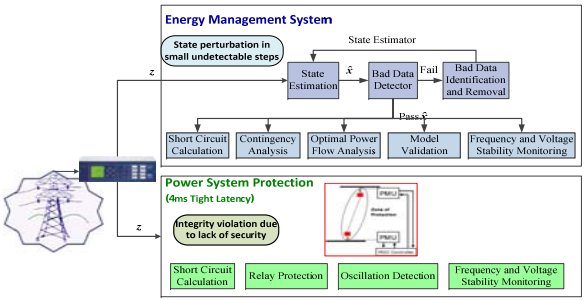
- Additive: Reports greater than actual power consumption
- Deductive: Reports lesser than actual power consumption
- Camouflage: Balance additive & deductive attacks from different meters
- Conflict: Unbalanced additive and deductive attacks from multiple uncoordinated adversaries

Anomaly Detection



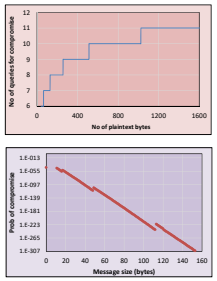
- A drop in the ratio of HM and AM is a reliable indication of occurrence of organized falsification
- Ratio are maintained as forgetting and cumulative moving averages
- The property holds for all types of attack and higher fractions of compromised nodes

Smart Grid Management

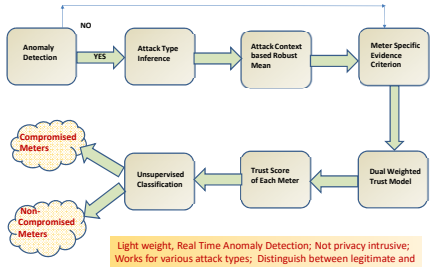


Security Analysis

- 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.

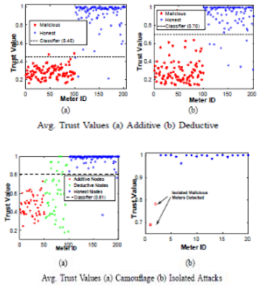


Proposed Framework: Overview



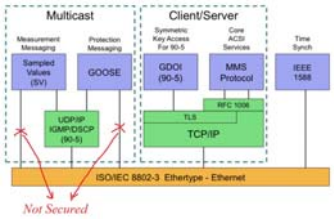
Light weight, Real Time Anomaly Detection; Not privacy intrusive; Works for various attack types; Distinguish between legitimate and malicious changes; Suitable for both isolated and organized rivals

Performance Evaluation



- We use Real Data Set from PECAN Street Project (SmartGridGov)
- We emulate attacks on real data fed to a virtual simulated AMI
- We observe clear difference between compromised and non-compromised nodes.
- Results are better due the robustness of statistical measures used in various steps
- Also works for isolated attacks

Communications & Security in IEC61850



Allowed values for MAC 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

Modules in green defined in 2012 standard, currently not deployed

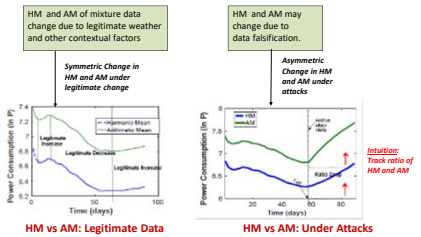
Performance Analysis

- 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

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

Legitimate and Malicious Changes

- Transform the observed data into a Gaussian mixture
- A light weight statistical indicator for anomalies: Harmonic to Arithmetic Mean ratio of the Gaussian Mixture



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 & 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