Bad Data Injection in Smart Grid: Attack and Defense Mechanisms

Presented by Bin Xie

R&D by Yi Huang

InfoBeyond Technology LLC

Agenda

- Introduction to Smart Grid
- Power System Model
- Bad Data Injection
- Defender Mechanism
  - Quickest Detection
- Attacker Learning Scheme
  - Independent Component Analysis
- Future Work
- Conclusions

Our Research and Products

❑ Research Highlights on Wireless Networks:

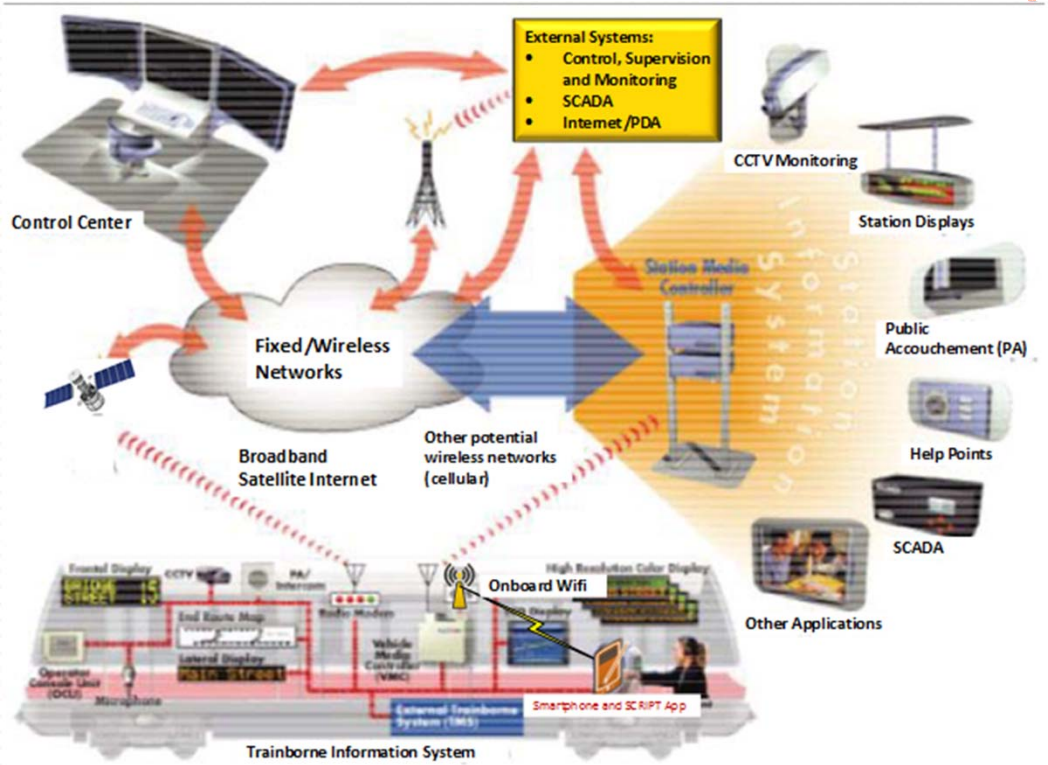
- **Network Delay and Reliability:**
  - Reducing Data Latency and Increasing Network Bandwidth and Reliability for Missile Defenses Using Network Coding
  - Network Coding and Network Tomography Analysis and Algorithms for Dynamic Airborne Networks
- **Spectrum Sensing and Allocations:** Efficient and Robust Dynamic Spectrum Access under Uncertainty
- **Interference Mitigation:** Efficient Range Segment Upgrade for Satellite Control Networks Using Stochastic Interference Prediction and Context-aware Smart Antenna Control

❑ Product Highlights:

- **Products are commercialization**

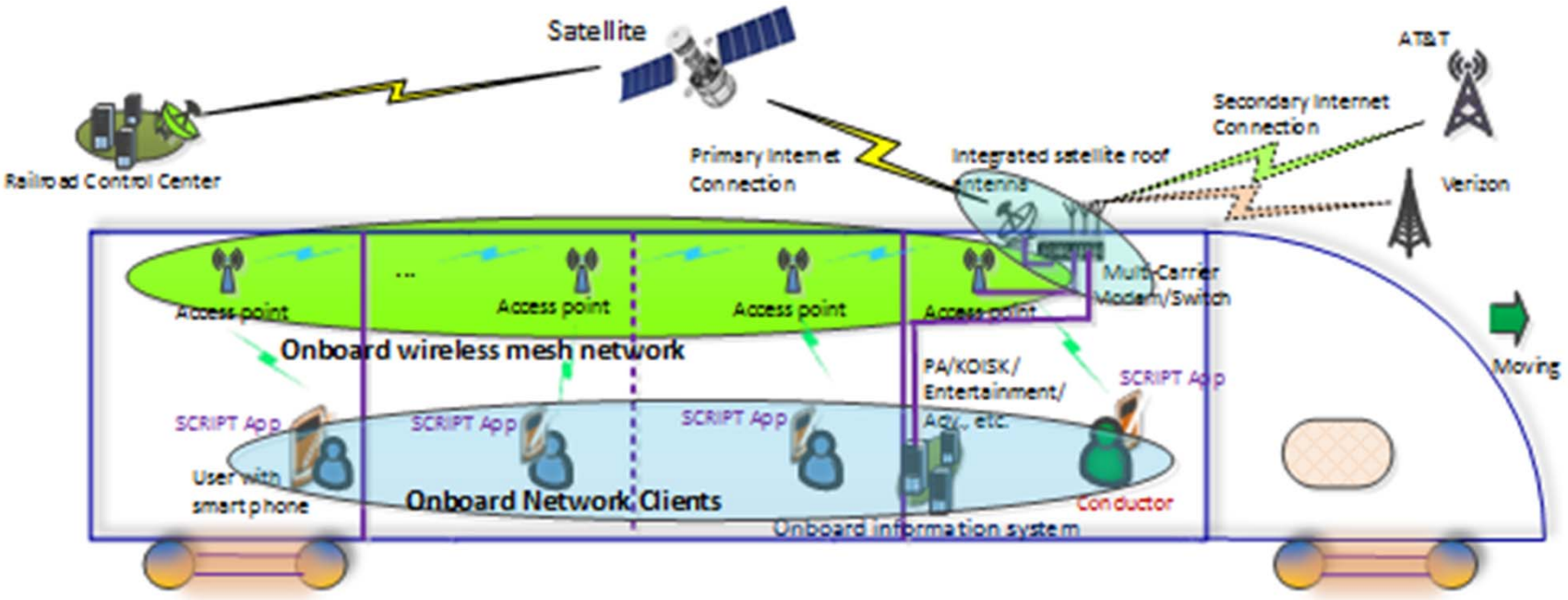
SMARTPHONE APPLICATION FOR ONBOARD RAILROAD PASSENGER INFORMATION SYSTEM

- **Railroad Data Communication**: Railroad broadband Internet networks is critical for providing PIS service. The mobility of trains requires a reliable wireless network providing both global Internet access and a onboard WLAN (e.g. WiFi)
- **Safety Response via Smartphones**: Disseminates security warning and instructions to passenger in real time fashion. Improve railroad safety management and security capabilities
- **Onboard Passenger Services** : Deliver real-time train status and ubiquitous trip information of the interest to passengers. Provide onboard service via passengers' smartphone.
- **Personalized Passenger Services** : Personalized trip planning, navigation, guidance between transfer points, rout, travelling groups, and reward programs for different types of passengers, e.g., triveller with children or infants, disabilities, etc.



Multimodal network and infrastructure environment in support of a PIS App for martphones or tablets

ALWAYS-ON RAILROAD NETWORKS ON THE MOVE



- **Satellite/Celluar Hybrid Global Internet**: Reliable network connectivity for onboard passenger services using commodity communication devices and services.
  - *Primary Satellite Broadband Internet*: large coverage, less handover, reliable
  - *Secondary Cellular High-speed Internet*: lower price, backup for bad weather, complex mountain terrain, tunnel, etc.
- **Onboard Train Mesh Network:** A set of wireless routers covering the train, self organization, self-healing, and self-configuration
- **Clients**: Using smartphone to access the global Internet through train Mesh network.

"Smarter" Power Grid

- Two-way realtime information & power-flow between utilities and consumers (e.g…supply vs. demand)
- More than 3.4 billion from US federal stimulus bill is targeted.
- Benefits both utilities, consumers,& environment:
  - Reduce supply while fitting demand
  - Save money, optimal usage.
  - Improve reliability and ffficiency of grid
  - Integration of green energy, reduction of CO_2
- One of hottest topic in research community
  - But what are the problems?

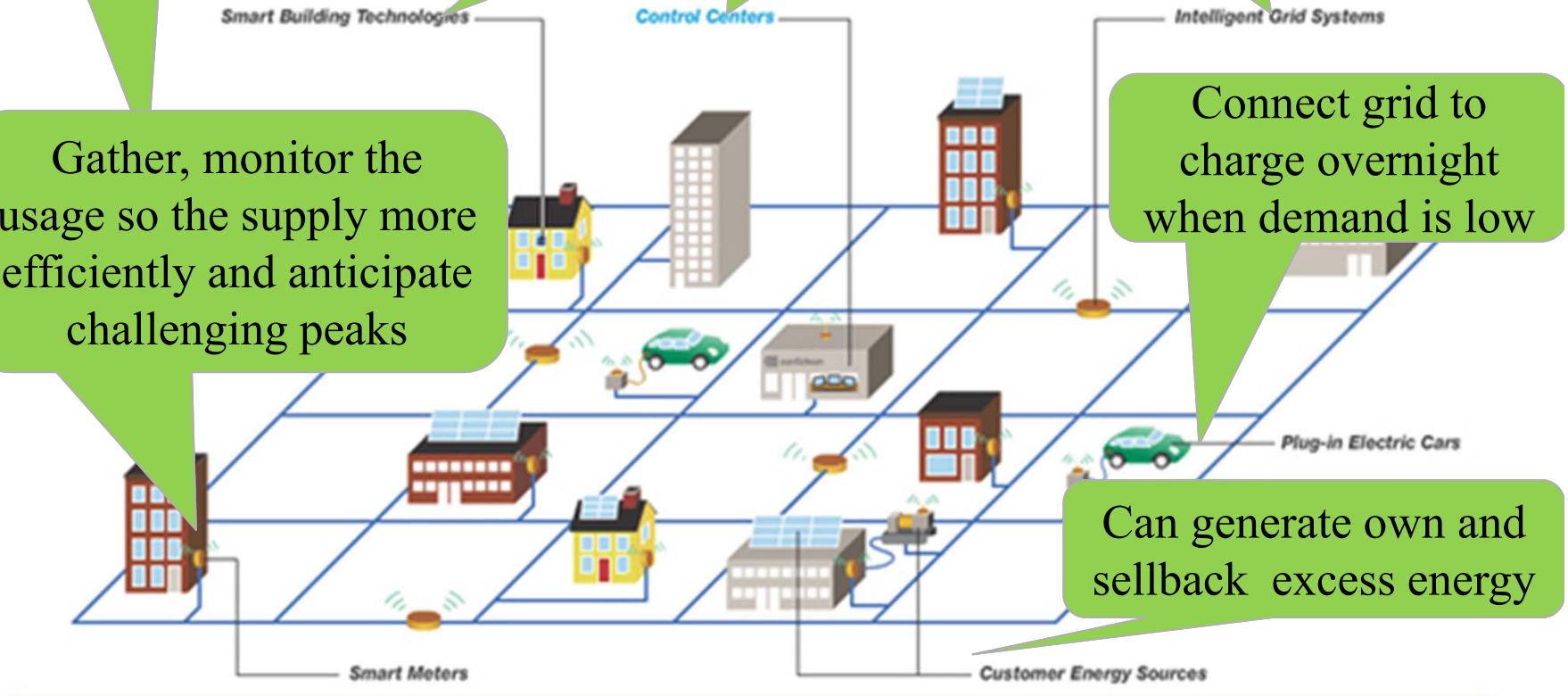
Let's view it graphically how everything is connected!

Are more easily integrated into power sys. Less depend on fossil fuel

Realtime analysis, Manage, plan, and forecast the energy

in-home management tool to track usage

Use sophisticated comm. Technology to find/fix problems faster, enhancing reliability



Gather, monitor the usage so the supply more efficiently and anticipate challenging peaks

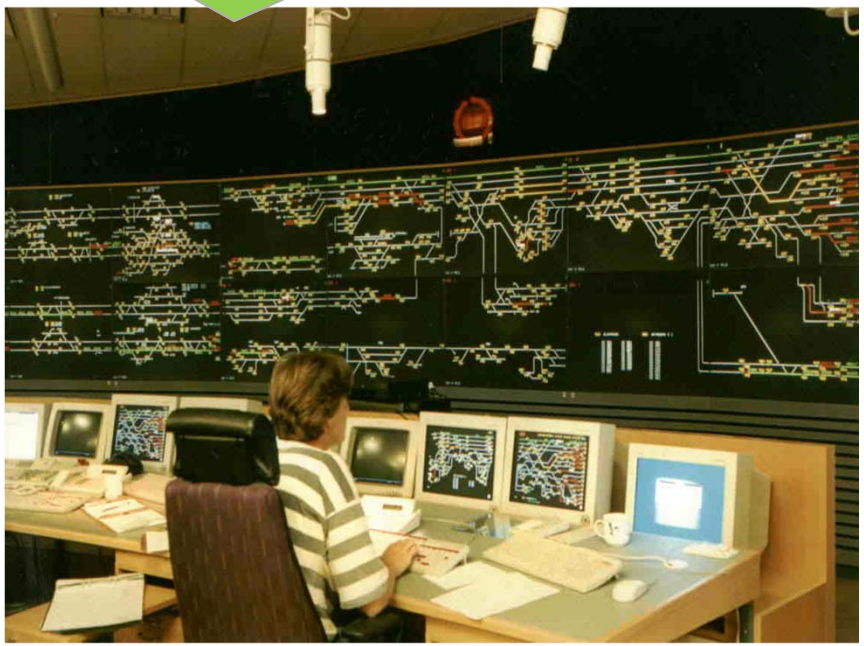
Connect grid to charge overnight when demand is low

Can generate own and sellback excess energy

Supervisory Control and Data Acquisition Center

- Real-time data acquisition
  - Noisy analog measurements
    - *Voltage, current, power flow*
  - Digital measurements
- State estimation
  - Maintain system in *normal* state
  - Fault detection
  - Power flow optimization
  - Supply vs. demand

SCDA TX data from/to Remote Terminal Units (RTUs), the substations in the grid



Privacy & Security Concern

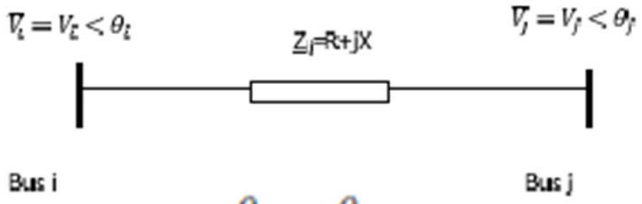
- More connections, more technology are linked to the obsolete infrastructure.
  - Add-on Network technology: sensors and controls est.
  - More substations are automated/unmanned
- It is vulnerable to manipulation by third party:
  - Purposely blackout
  - Financial gain
- National security, safety-critical, and huge economic damages
- Electricity generation, electricity transmission and distribution
- Cyber grid security is the most pressing sector issues of 2017

How to tackle this cybersecurity vulnerability?

Power System Model

- Transmitted active power from bus i to bus j
  - High reactance over resistance ratio

$$P_{ij} = \frac{V_i V_j}{X_{ij}} \sin(\theta_i - \theta_j)$$



  - Linear approximation for small variance $P_{ij} = \frac{\theta_i - \theta_j}{X_{ij}}$
  - State vector $\mathbf{x} = [\theta_1, \ldots, \theta_n]^T$, measure noise **e** with covariance Σe
  - Actual power flow measurement for m active power-flow branches

$$\mathbf{z} = \mathbf{P}(\mathbf{x}) + \mathbf{e}$$

  - Define the Jacobian matrix $\mathbf{H} = \frac{\partial \mathbf{P}(\mathbf{x})}{\partial \mathbf{x}} |_{\mathbf{x}=\mathbf{0}}$
  - We have the linear approximation

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{e}$$

  - H is known to the power system but not known to the attackers

State estimation (SE)

z=Hx+e, for n power lines and m measurement, m<n

H: Jacobean Matrix (n×n)

x: State variable (n×1)

z: Measurements (m×1)

e: noise vector (n×1)

- Goal of system is to estimate **x** from **z**

$$\hat{\mathbf{x}} = (\mathbf{H}^T \boldsymbol{\Sigma}_e^{-1} \mathbf{H})^{-1} \mathbf{H}^T \boldsymbol{\Sigma}_e^{-1} \mathbf{z}.$$

- SE is a key function in building real-time models of electricity networks in Energy Management Centers (EMC)
- Real-time models of the network can be used by Independent System Operator (ISO) to make optimal decisions with respect to technical constraints (such as transmission line congestion, voltage and transient stability)

Bad Data Injection and Detection

- Inject Bad data c: **z=Hx+c+e**
- Bad data detection
  - Residual vector $\mathbf{r} = \mathbf{z} - \mathbf{H}\hat{\mathbf{x}}$
  - Without attacker $E(\mathbf{r}) = 0 \quad cov(\mathbf{r}) = (\mathbf{I} - \mathbf{M})\mathbf{\Sigma}_e$

    where $\mathbf{M} = \mathbf{H}(\mathbf{H}^T\mathbf{\Sigma}_e^{-1}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{\Sigma}_e^{-1}$
  - Bad data detection (with threshold γ)

    without attacker: $\max_i |r_i| \leq \gamma$

    with attacker: otherwise
- Stealth (unobservable) attack

$$\mathbf{z}' = \mathbf{H}(\mathbf{x} + \delta\mathbf{x}) + e$$

  - Hypothesis test would fail in detecting the attacker, since the control center believes that the true state is x + δx.

Overview

- Introduction to Smart Grid
- Power System Model
- Bad Data Injection
- Defender Mechanism
  - Quickest Detection
- Attacker Learning Scheme
  - Independent Component Analysis
- Future Work
- Conclusions

Basics of Quickest Detection (QD)

- A technique to detect distribution changes of a sequence of observations as quick as possible with the constraint of false alarm or detection probability.
- Decoding on-line information in a way that minimizes the delay between the time a change occurs and the time it is detected, while maintaining a certain level of detection accuracy

  min [processing time]

  s.t. Prob(true ≠ estimated) < ŋ

- An implementable, real-time signal analysis detection tool
  - Information can be updated in time before failure

Classification of Quickest Detection

- **Sequential analysis for change detection**

1. *Bayesian framework:*

   at random time (known distributions), detect distribution changes between two known distribution.

   - known prior probability
   - SPRT –Sequential probability ratio test (e.g. quality control, drug test,)

2. *Non-Bayesian framework:*

   at random time (unknown distribution), detect distribution changes to known/unknown distribution.

   - CUSUM – Cumulative sum control chart (e.g. spectrum sensing, abnormal detection)

QD System Model

- Assuming Bayesian framework:
  - the state variables are random with $\mathcal{N}(\mu_z, \Sigma_z)$
- The binary hypothesis test:

$$\mathcal{H}_0 : \mathbf{a} = 0 \quad \text{vs.} \quad \mathcal{H}_1 : \mathbf{a}$$

- The distribution of measurement z under binary hyp: (differ only in mean)

$$\begin{aligned} \mathcal{H}_0 &: \mathbf{z} \sim \mathcal{N}(\mathbf{0}, \Sigma_z) \\ \mathcal{H}_1 &: \mathbf{z} \sim \mathcal{N}(\mathbf{a}, \Sigma_z), \end{aligned} \quad \text{where } \Sigma_z \triangleq \mathbf{H}\Sigma_x\mathbf{H}^{\mathrm{T}} + \Sigma_e$$

- We want a detector $\delta(\mathbf{z}) \in \{0, 1\}$
  - False alarm and detection probabilities

$$P_F = \Pr(\delta(\mathbf{z}) = 1|\mathcal{H}_0), \quad P_D = \Pr(\delta(\mathbf{z}) = 1|\mathcal{H}_1)$$

Detection Model - NonBayesian

- Requiring a Non-Bayesian approach due to unknown prior probability, attacker statistic model
- The unknown parameter exists in the post-change distribution and may changes over the detection process. You do not know how attacker attacks.
- Minimizing the worst-case effect via detection delay:

Detection delay | Detection time | Actual time of active attack

$$T_d = \sup_{\tau \geq 1} E_\tau [T_h - \tau | T_h \geq \tau]$$

- We want to detect the intruder as soon as possible while maintaining $P_{D.}$
- Important in practice

Multi-thread CUSUM Algorithm

- CUSUM Statistic:

$$S_t = \max_{1 \geq k \geq T_h} \sum_{t=k}^{T_h} L_t,$$

How about the unknown?

where Likelihood ratio term of *m* measurements:

$$L_t(\mathbf{Z}_t) = \sum_{l=1}^{m} \log \frac{f_1(\mathbf{Z}_t | a_{t,l})}{f_0(\mathbf{Z}_t)}, \qquad \mathbf{Z}_t \ (z_{t,l}, l \in 1, 2, \cdots, m)$$

- By recursion, CUSUM Statistic S_t at time t:

$$S_t = \max(S_{t-1}, 0) + L_t(\mathbf{Z}_t), \quad \text{where } S_0 = 0.$$

- Average run length (ARL) for declaring the attack:

$$T_h = \inf\{t \geq 1 | S_t > h\},$$

Declare the attacker is existing!

Otherwise, continuous to the process.

Linear Solver for the unknown

- Rao test – asymptotically equivalent model of GLRT:

at time t, $\mathbf{Z}_t \in \{z_{t,l}\}$, and $\mathbf{a}_t \in \{a_{t,l}\}$ where $l = 1, 2, \cdots, m$.

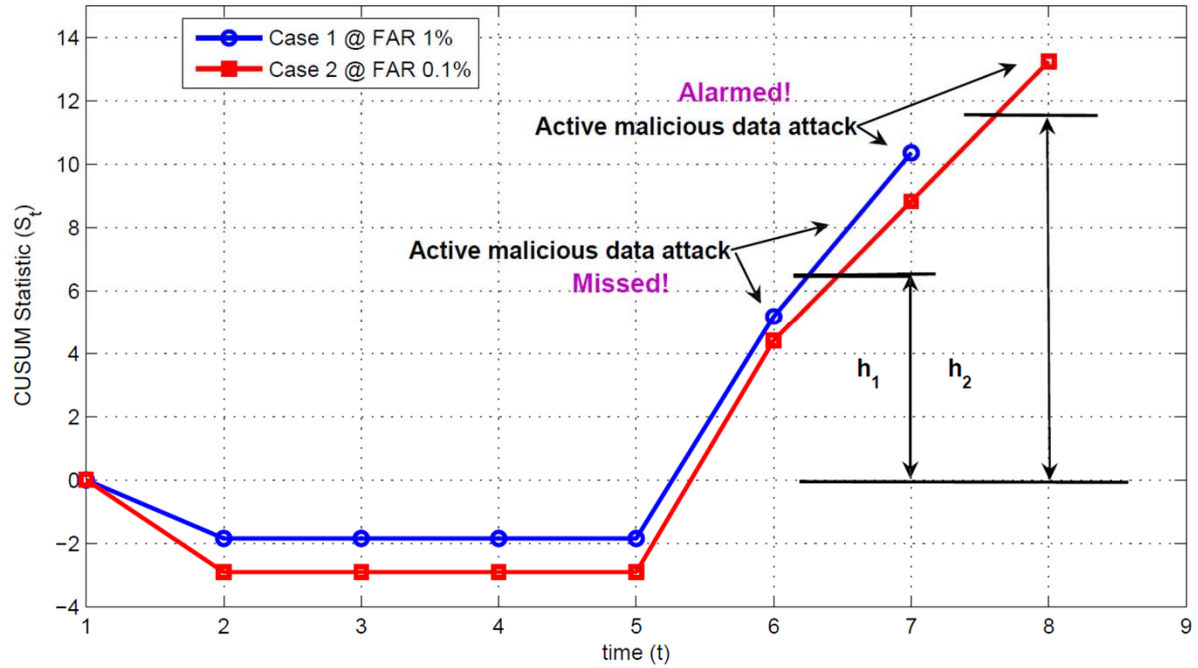
$$\mathcal{R}(\mathbf{Z}_t) = \frac{\partial \log[f_1(\mathbf{Z}_t|\mathbf{a}_t)]}{\partial \mathbf{a}_t}\bigg|^{T}_{\mathbf{a}_t=\hat{\mathbf{a}}_t^0} \quad [\mathbf{J}^{-1}(\hat{\mathbf{a}}_{tt}^{\,0})]_{\mathbf{a}} \frac{\partial \log[f_1(\mathbf{Z}_t|\mathbf{a}_t)]}{\partial \mathbf{a}_t}\bigg|_{\mathbf{a}_t=\hat{\mathbf{a}}_t^0},$$

- The linear unknown solver for m measurements:
  - Omitting the necessity of [J-1] ➡ solo-parameter envir.
  - Simplifying Quadratic form ➡ the unknown > 0
- Recursive CUSUM Statistic w/ linear unk

The unknown is no long involved

$$S_t = \max(S_{t-1}, 0) + \sum_{l=1}^{m} \left[(\mathbf{Z}_t^T \boldsymbol{\Sigma}_z^{-1})^T + \boldsymbol{\Sigma}_z^{-1}\mathbf{Z}_t\right].$$

Simulation: Adaptive CUSUM algorithm



- 2 different α–leave detection tests: FAR: 1% and 0.1%
- Active attack starts at time 6
- Missing detection occurs; two different thresholds

Overview

- Introduction to Smart Grid
- Power System Model
- Bad Data Injection
- Defender Mechanism
  - Quickest Detection
- Attacker Learning Scheme
  - Independent Component Analysis
- Future Work
- Conclusions

Independent Component Analysis (ICA)

- Linear ICA is a recently developed method in which the goal is to find a linear representation of the data so that components are as statistically independent as possible.
  - Among the data, find how many independent sources.
- **Question:**
  - Without knowing **H**, the attacker can be caught.
  - Could Attacker, stealthy attack to the system even without knowledge about **H**?
  - This work shows that, using ICA, Attacker could estimate **H** and consequently, lunch an undetectable attack.

$$\mathbf{z}' = \mathbf{H}(\mathbf{x} + \delta\mathbf{x}) + e$$

ICA Basics

- Linear ICA: separating a multivariate signal into subcomponents using statistical independence of the non-Gaussian source signals
- A special case of blind source separation

$$\mathbf{u} = \mathbf{G}\,\mathbf{v}$$

- $\mathbf{u} = [u_i, i = 1, 2, \ldots m]$: observable vector
- $\mathbf{G} = [g_{ij}, i = 1, 2, \ldots m, j = 1, 2, \ldots n]$: mixing matrix (unknown)
- $\mathbf{v} = [v_i, i = 1, 2, \ldots n]$: source vector (unknown)

Stealth False Data Injection with ICA

- Supposing that the noise is small, then we what to do the mapping:

$$\mathbf{u} = \mathbf{G}\,\mathbf{v} \longrightarrow \mathbf{z} = \mathbf{H}\,\mathbf{x}$$

- Problem: state vector **x** is highly correlated
- Consider: **x = A y**, where
  - **A**: eigenvectors of **x**
  - **y**: independent random vectors
- Then we can apply Linear ICA on **z = HA y**
- Linear ICA implementation: FastICA from [Hyvärinen]

Algorithm

Algorithm 1: Stealth false data injection

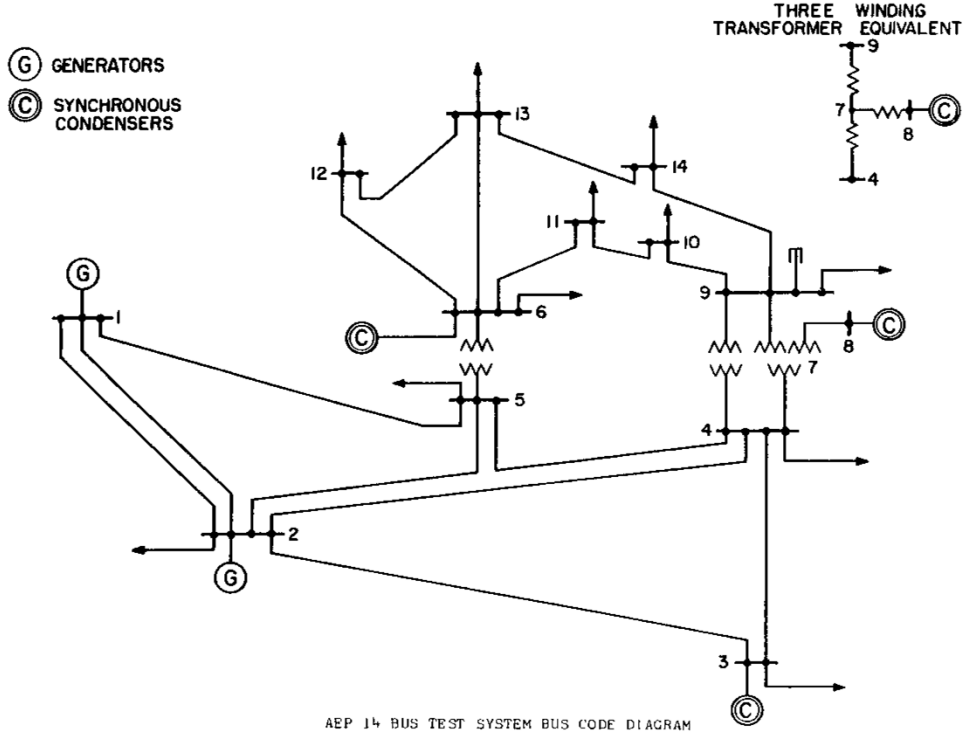
input : $\mathbf{z}$ = data matrix;

1 [$\mathbf{G}$ and $\mathbf{y}$] = `FastICA` ($\mathbf{z}$);
2 **if** $\max(\mathbf{z} - \mathbf{G}\mathbf{y}) > \epsilon$ **then**
  exit;
3 Generate $\delta\mathbf{y} \sim N(0, \sigma^2)$;
4 $\mathbf{z}' = \mathbf{z} + \mathbf{G}(\mathbf{y} + \delta\mathbf{y})$;

output: false data $\mathbf{z}'$

Numerical Setting

- The presented results are experiment results conducted on 4-Bus test system, IEEE 14-Bus and 30-bus smart grid models with different number of measurements.
- Modeling Electrical loads as Random variables and, running power flow program in Matpower, will provide us random measurements Z.

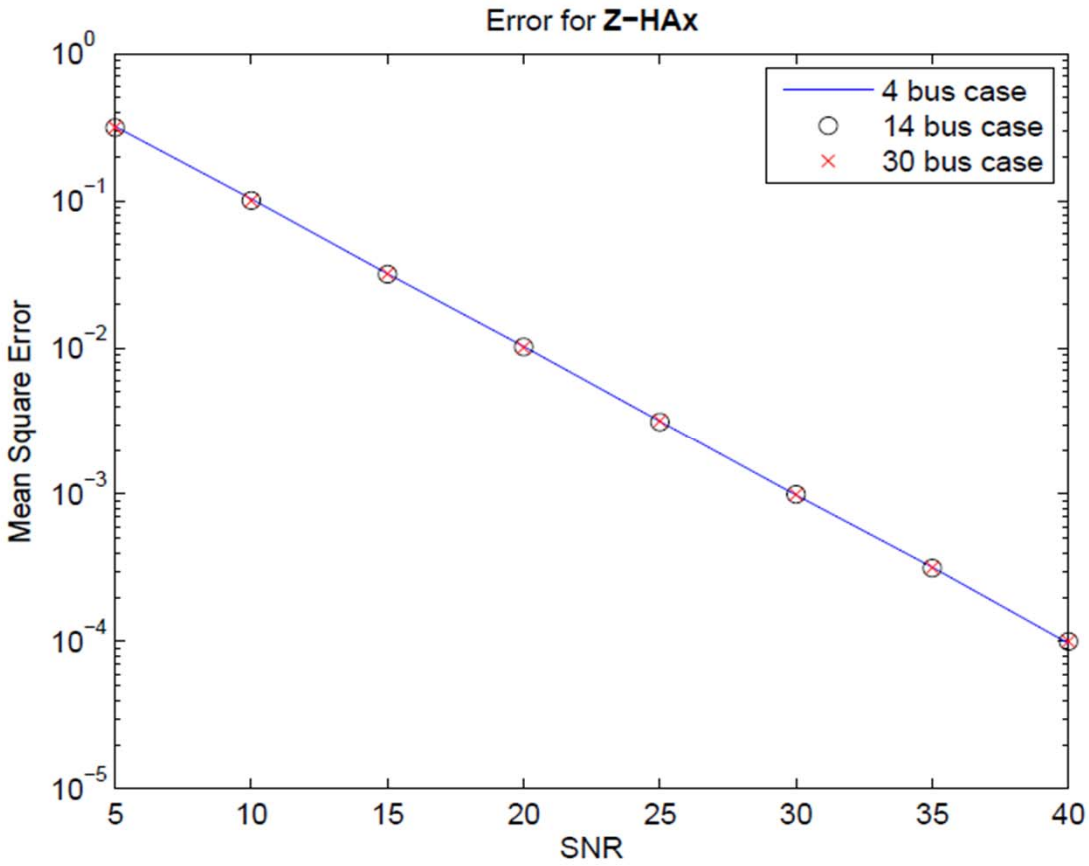


Numerical results

- **Validation of linearity in ICA**

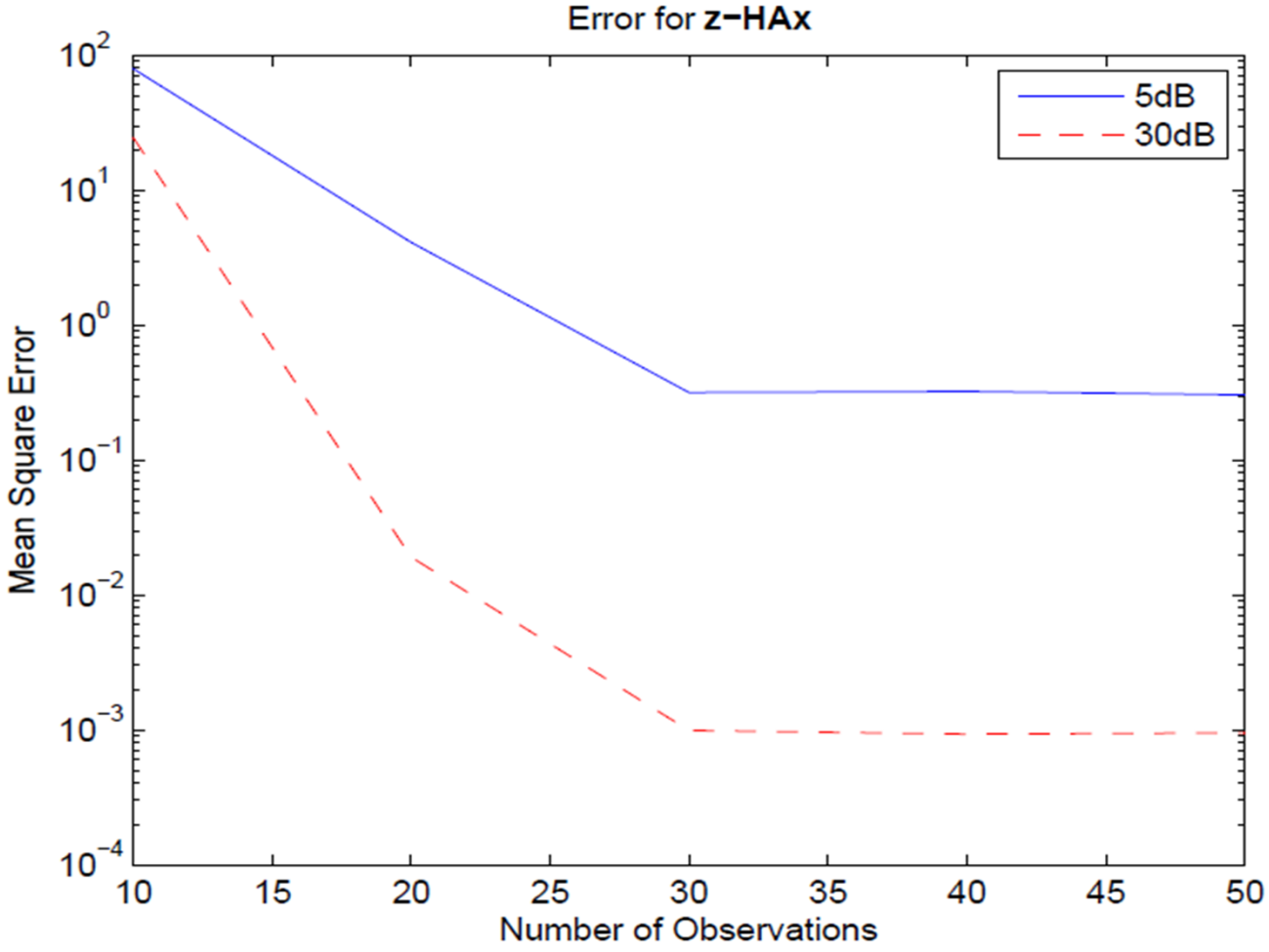
  Evaluation of linearity assumptions in ICA and its performance with different levels of noises and the number of measurements.

MSE of ICA inference (z-Gy) vs. SNR.

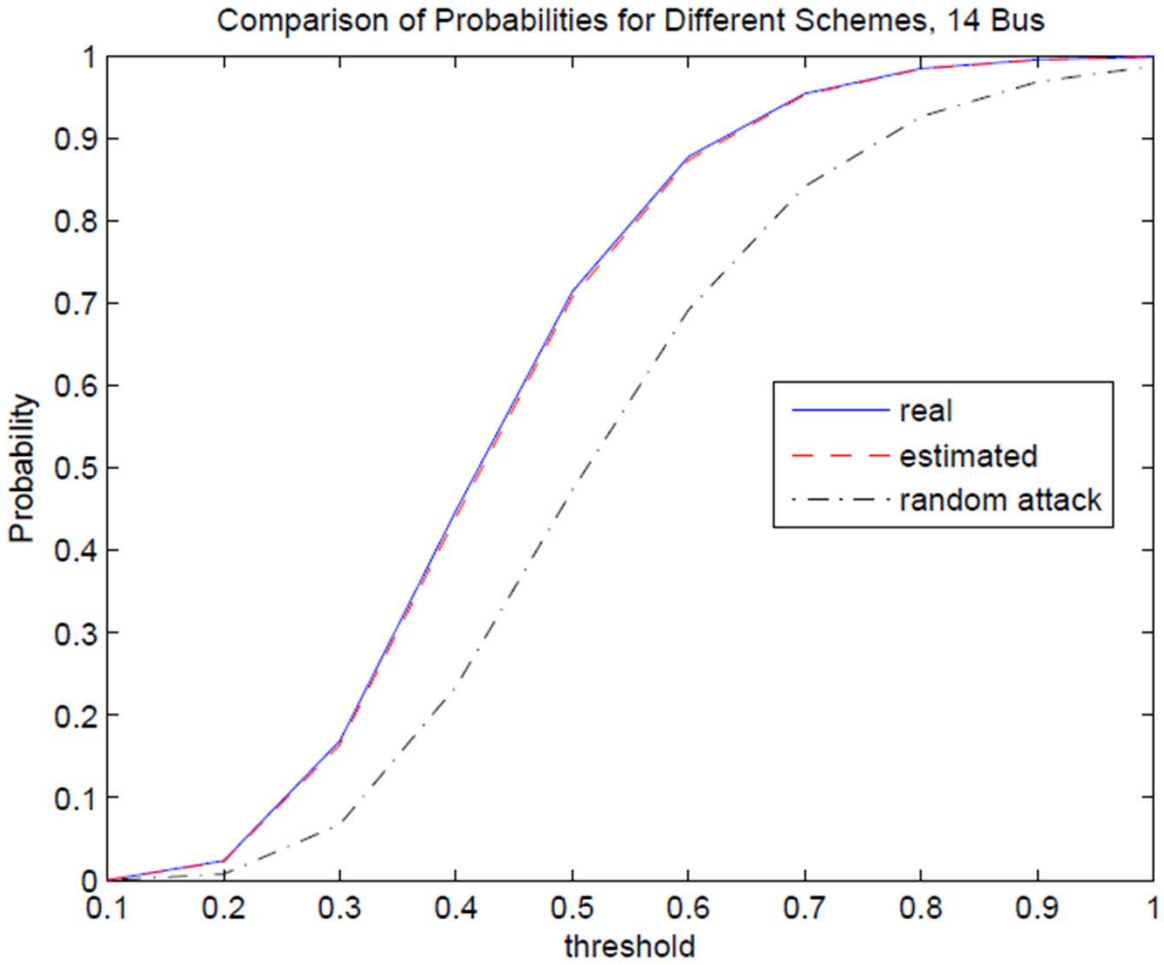


Numerical results

- MSE of ICA inference (z-Gy) vs. the number of observations (14-bus case).



Performance of the attack



Probability for miss detection of attacks

Overview

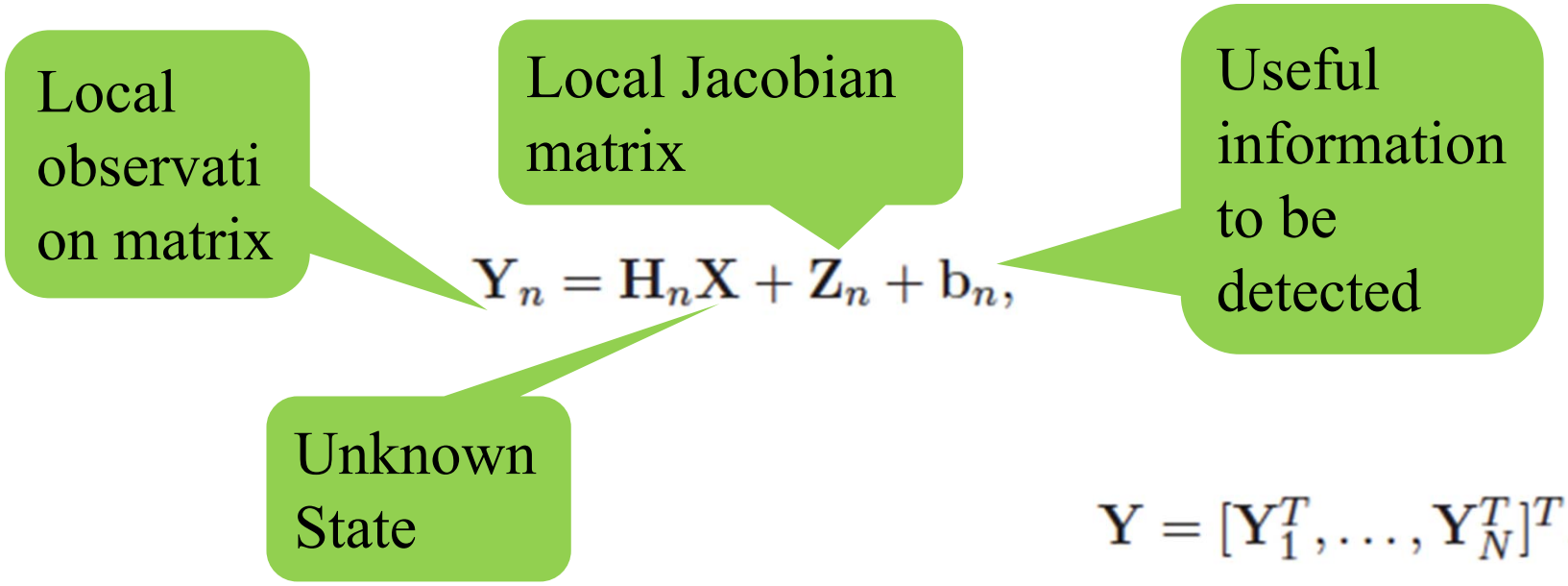
- Introduction to Smart Grid
- Power System Model
- Bad Data Injection
- Defender Mechanism
  - Quickest Detection
- Attacker Learning Scheme
  - Independent Component Analysis
- Future Work
- Conclusions

1. Distributed Smart Grid State Estimation

- The deregulation has led to the creation of many regional transmission organizations within a large interconnected power system.
- A distributed estimation and control is need .
  - Distributed observability analysis
  - Bad data detection
- Challenges:
  - bottleneck and reliability problems with one coordination center.
  - need for wide area monitoring and control
  - D-SG statistic convergence to C-SG

Fully-Distributed State Estimation

- By iteratively exchanging information with neighboring control areas, all local control areas can achieve an unbiased consensus of system-wide state estimation.
- With N substations/nodes,



2. Optimality of fault detection algorithm

- Detecting the attack as an intermediate step towards obtaining a reliable estimate about the injected false data
  - which in turn facilitates eliminating the disruptive effects of the false data
- Assuring good estimation performance is the core of estimation and detection problem
- We want
  - Define an estimation performance measure
  - Seek to the optimize it while ensuring satisfactory of the detection performance

Optimality of fault detection algorithm

- We formulate the optimization problem:
  –

$$\min_{\delta_0,\delta_1,\hat{\mathbf{b}}} \quad J(\delta_0,\delta_1,\hat{\mathbf{b}}),$$

$$s.t. \quad \text{FAR} \le \alpha$$
$$\text{MDR} \le \beta,$$

Performance measurement

  – By applying the minimum-square error (MSE)/P_D+C_1P_f+C_2P_m,

$$\text{MSE} : C(\mathbf{b},\hat{\mathbf{b}}(\mathbf{y})) = ||(\mathbf{b}-\hat{\mathbf{b}}(\mathbf{y})||^2,$$

Other Future Work

- Formulate the damage of bad data injection
  - E.g. Market price. Le Xie
- Joint estimation and detection problem
  - Some work from Princeton
- Other learning methods beyond ICA
- Analysis of interactions between attackers and defenders
  - Game theoretical point of view
- Collusion attack
- Cooperative defense

Conclusion

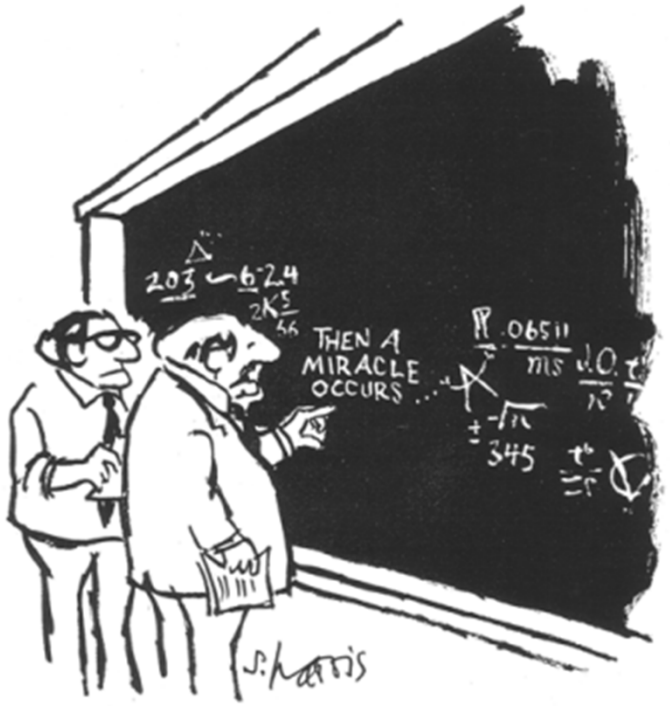
- Bad data injection problem formulation
- From defender point of view
  - The implementable defense strategy for malicious data attack in Smart Grid State Estimation.
  - Adaptive CUSUM algorithm
- From attacker point of view
  - We showed that an attacker can estimate both the system topology and power states just by observing the power flow measurements.
  - Once the information is at hand, malicious attacks can be launched without triggering the detection system. Independent component analysis algorithm is proposed to obtain the information.

Our Research and Development

Technical Highlights:

- Satellite Control Network – Smart Antenna Control
- Wireless Mesh Networks – High Speed Data Local Networks
- Networks and Security
- Cloud, and
- Big Data & Machine Learning
- www.InfoBeyondtech.com
- www.NXdrive.com
- www.Securitypolicytool.com

THANK YOU!



"I THINK YOU SHOULD BE MORE EXPLICIT HERE IN STEP TWO."