A Quickest Detection Framework for Smart Grid

Ph.D. Defense
Yi Huang

Adviser: Prof. Zhu Han
Wireless Networking, Signal Processing and Security Lab
Electrical and Computer Engineering Department
University of Houston
11-30-2012

Outline

- Introduction
  - What's Smart Grid?
  - Motivation for Quickest Detection (QD)
- Accomplishments
  - Real-Time Detection of False Data Injection in Smart Grid Networks: An Adaptive CUSUM Method and Analysis
  - Adaptive Quickest Estimation Algorithm for Smart Grid Network Topology Error
  - Online Quickest Multiarmed Bandit Algorithm for Distributive Renewable Energy Resources
- Summary
- Future work

What is Smart Grid?

Sensors thru. out

pervasive control

Self-healing/monitoring

Digitalization

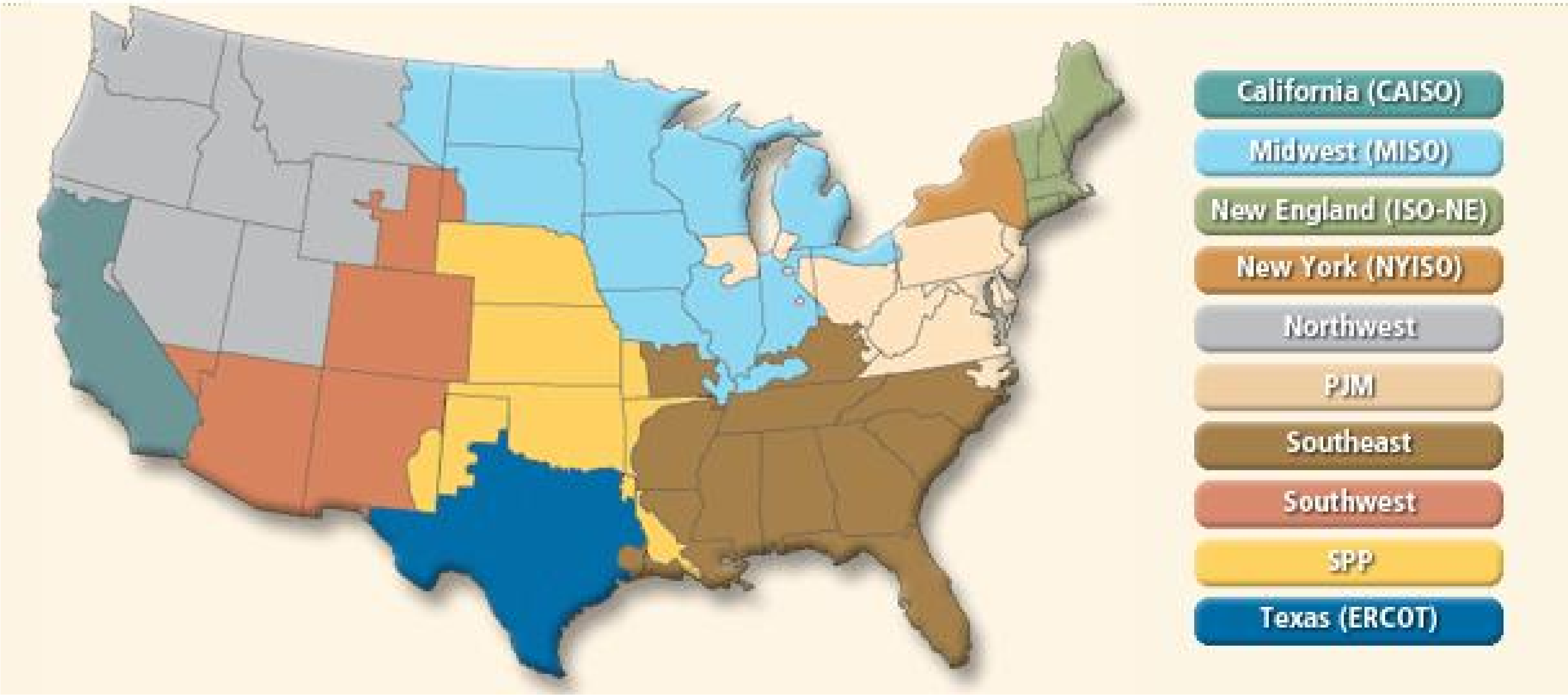
Centralized vs. distributed

2 way flow info & elec

More choices for endusers

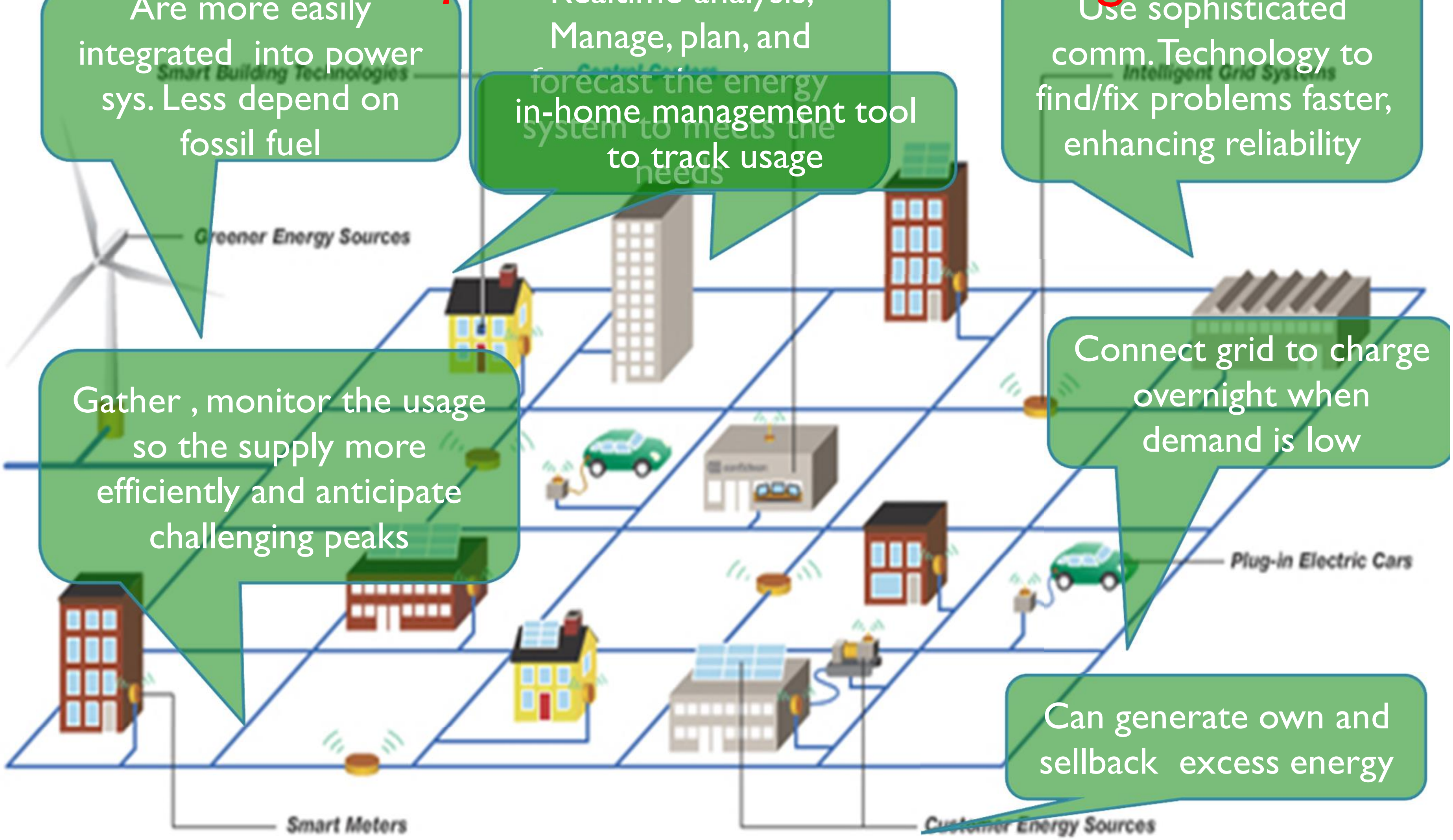
[10] N. I. of Standards and Technology, "Nist framework and roadmap for smart grid interoperability standards," *National Institute of Standards and Technology Report, release 1.0*, no. 1, Jan 2010.

Smart Grid - Regional Electricity Markets



In 2001, *DOE* began studying on distr. energy integration.
In 2007, *Energy Independence & Security Act* focus on SG R&D
In 2009, *American Recovery & Reinvestment Ac*t brings SG 3.4 billion

Advance infrastructure is a double-edge sword!



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

Realtime analysis, Manage, plan, and forecast the energy system to meets the needs

in-home management tool to track usage

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

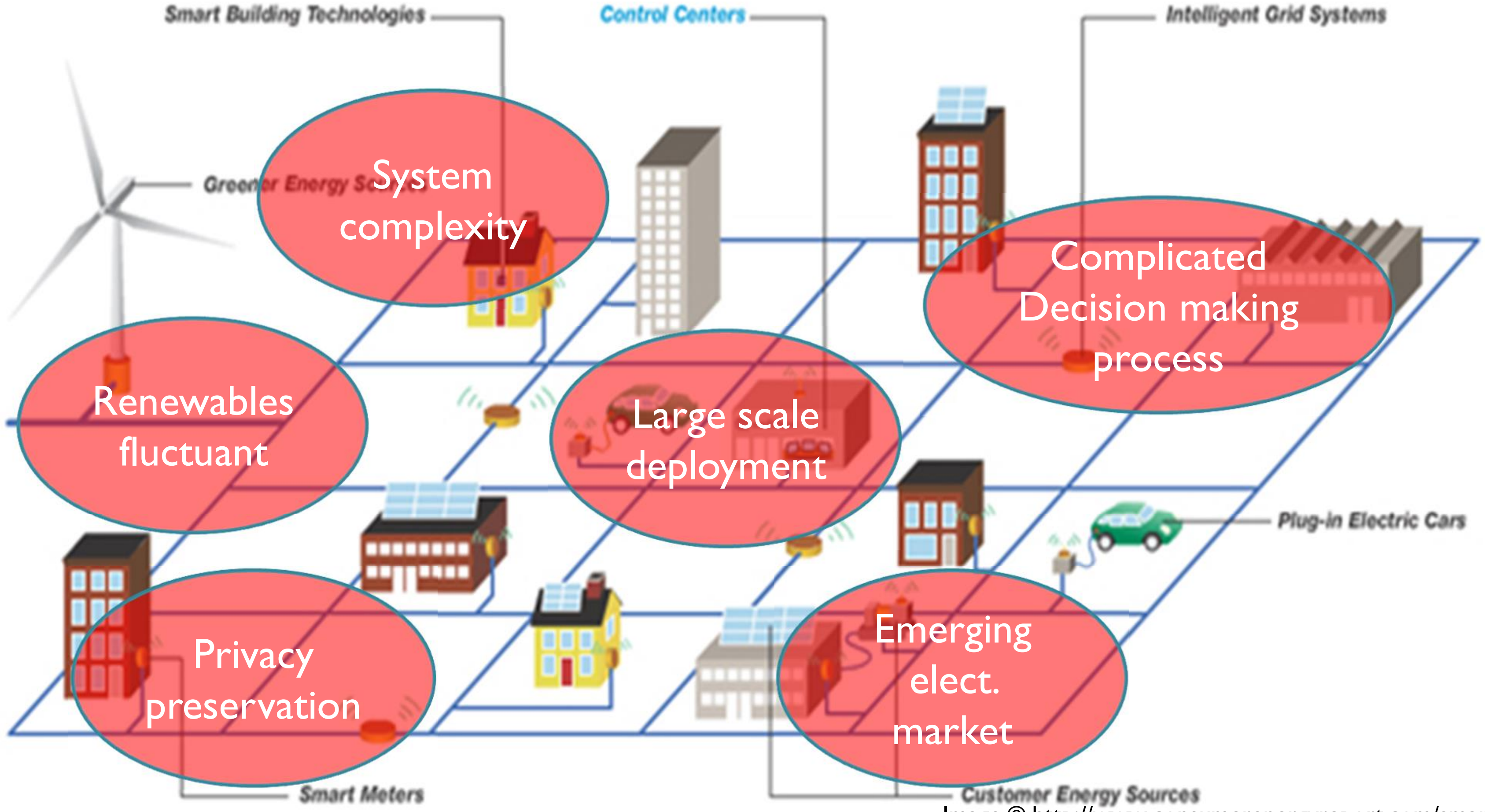
Gather , monitor the usage so the supply more efficiently and anticipate challenging peaks

Connect grid to charge overnight when demand is low

Can generate own and sellback excess energy

Image © http://www.consumerenergyreport.com/smart-grid/

Challenges in SG



System complexity

Complicated Decision making process

Renewables fluctuant

Large scale deployment

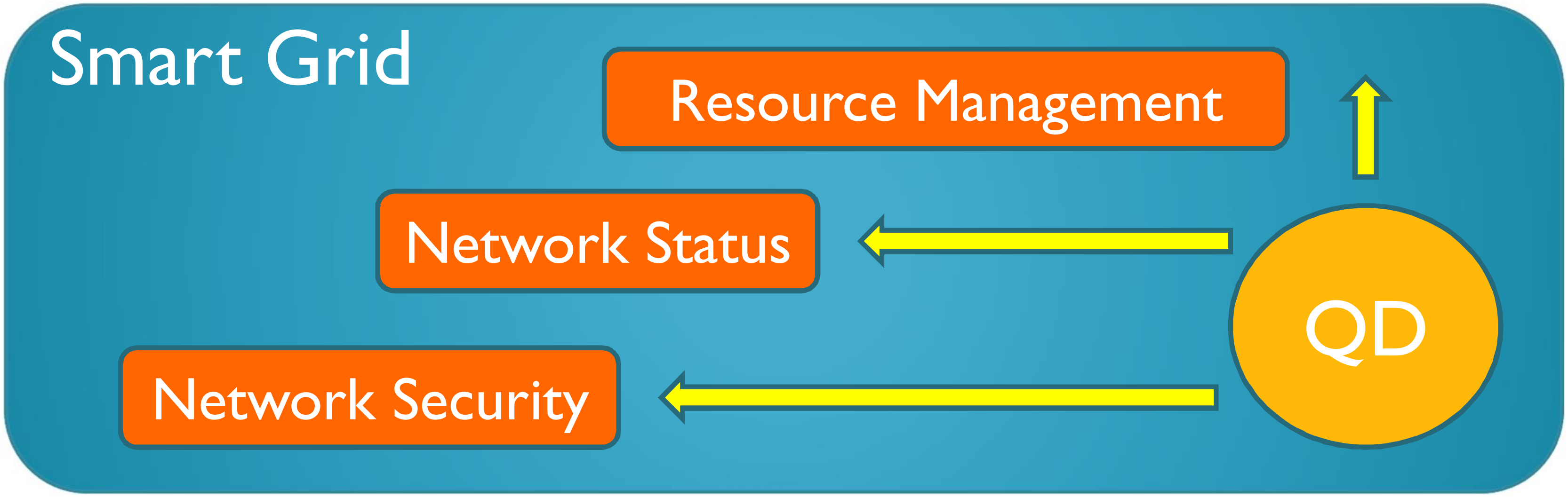
Privacy preservation

Emerging elect. market

Image © http://www.consumerenergyreport.com/smart-grid/

QD Techniques in SG

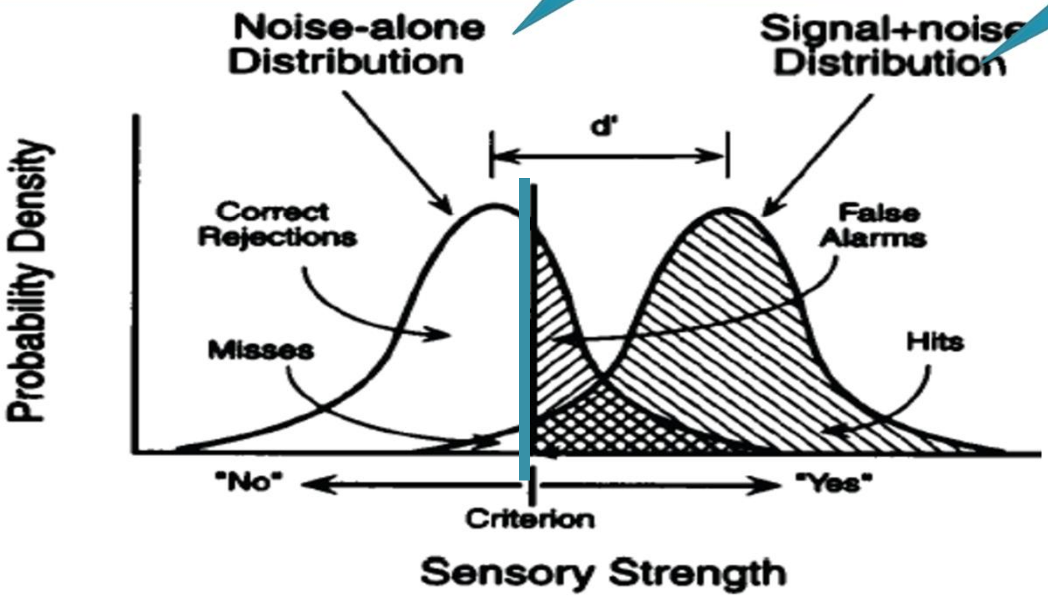
- Delay-sensitive, high security req., complex system, unpredictable DGs, etc.
- An objective is to response events promptly to help prevent catastrophic failures
-



Basic QD: Statistical Hypothesis Test

H0: y(t)=n(t)

H1: y(t)=h(t)+n(t)



- The optimal decision is given by the Likelihood ratio test:

  Select H1 if L(y) = log(P(y|H1)/P(y|H0)) > a criterion;

  otherwise select H0.

Why Quickest Detection?

- A implementable realtime signal analysis detection/decision tool
- Decoding on-line information in a way of:
  - minimizing the delay btw. t_{change} and t_{detect}
  - maintaining a certain level of detection accuracy
  - min [processing time],

    s.t. Prob. error < ŋ

Different from traditional detection methods

* The classical methods focus on fixed sample size, and error probabilities usually are not guaranteed.

Classification of QD

- Bayesian framework:
  - At random time, detect distribution between known distributions.
  - known prior information
  - SPRT
    - e.g. quality control, drug test, 2 known conditions (good or bad)
- Non-Bayesian framework:
  - At random time, detect distribution changes to known/unknown distribution.
  - CUSUM
    - e.g. spectrum sensing, *abnormal detection, (blinded on other side)*

Outline

- Introduction
  - What's Smart Grid?
    - Legislations, Programs, Standards
    - Structure Overview and Challenges
  - Motivation for Quickest Detection
- Accomplishments
  - **Real-Time Detection of False Data Injection in Smart Grid Networks: An Adaptive CUSUM Method and Analysis**
  - Adaptive Quickest Estimation Algorithm for Smart Grid Network Topology Error
  - Online Quickest Multiarmed Bandit Algorithm for Distributive Renewable Energy Resources
- Summary
- Future work

Main Contributions

- CUSUM-based defense algorithm for false data injection attack
  - A sequence of measurements lead more reliable decisions than using only snapshot measurements in SE.
  - Low complexity approach for solving unknown
- Fit for any applications of change point detection/decision
  - to detect the presence of attacks in that the pdf of the post-change is unknown.
- Flexible for modification and simplification
  - Easily extended to detect various other kinds of abnormal changes.
- Major publication
  - Accepted, IEEE Communications Magazine: Cyber Security Smart Grid Series
  - Major revision, IEEE Transactions on Smart Grid: Cyber and physical security systems

Power System Monitoring

- State Estimation (SE): Estimation of states over the power grid using redundant measurements.
- How does control center conduct SE?

  Supervisory Control and Data Acquisition (SCADA) system

Control Center

Communication
(DNP3)

Remote Terminal Unit

Measurements

State Estimation (SE)

Communication could be wireless (e.g., radio, and pager) or wired (e.g., Dial-up telephone, RS-485 multi-drop, 3G, and Ethernet).

- SE is vulnerable to cyber attack

These communication links are vulnerable to cyber attack.

Maroochy waste water utility

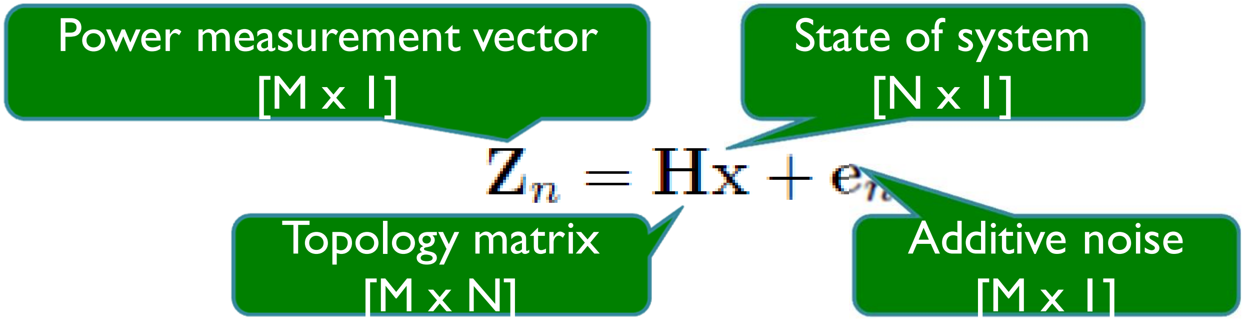
Unauthorized access to the control system via an insecure wireless network.

Olympic pipeline company

A system administrator was doing development on live SCADA

SE in SG

- Power model:



Power measurement vector [M x 1]

State of system [N x 1]

$$\mathrm{Z}_n = \mathrm{H}\mathrm{x} + \mathrm{e}_n$$

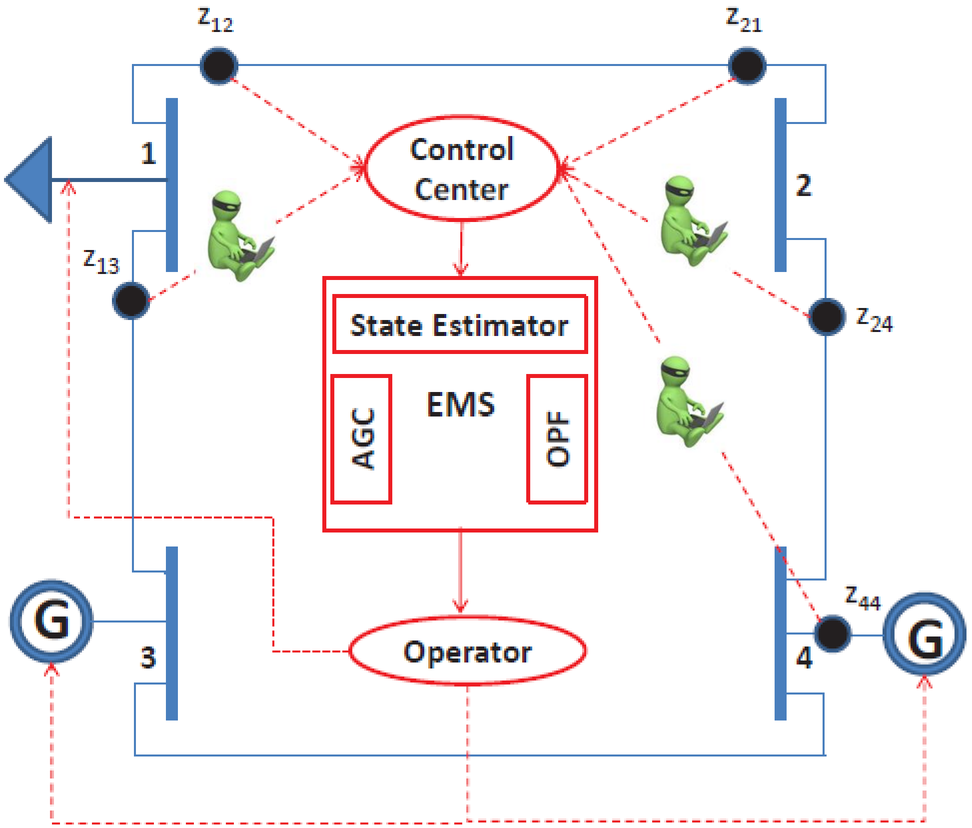
Topology matrix [M x N]

Additive noise [M x 1]

  - Size of **Z** >> size of **x.** (adv. of matrix redundancy)
  - Applying WLS, estimated system state $\hat{\mathrm{x}} = (\mathrm{H}^T \Sigma_e^{-1} \mathrm{H})^{-1} \mathrm{H}^T \Sigma_e^{-1} \mathrm{Z}_n$
- Bad date processer computes residual : $\mathrm{R}_n = \mathrm{Z}_n - \hat{\mathrm{Z}}_n$
  - $\hat{\mathrm{Z}}_n = \mathrm{H}\hat{\mathrm{x}} = \mathrm{H}(\mathrm{H}^T \Sigma_e^{-1} \mathrm{H})^{-1} \mathrm{H}^T \Sigma_e^{-1} \mathrm{Z}_n = \Im \mathrm{Z}_n$
  - $E(\mathrm{R}_n) = 0$ then x can be used for SG OPF, AGC, EMS, etc
  - otherwise, it is bad data, remove z, estimate again

False Data Attack

- Unknown time, prior prob. of adversary



Problem Formulation

- Under bad data, power measurements Z is

$$\mathbf{Z}_n = \mathbf{H}\mathbf{x} + \enclose{circle}{\mathbf{b}_n} + \mathbf{e}_n. \quad \text{where} \quad \mathbf{a}_n = \Im \mathbf{b}_n$$

Unknown mean vector a_n

- Using residual R to forms SHT:

$$\mathbf{R}_n = \mathbf{Z}_n - \hat{\mathbf{Z}}_n \Longrightarrow \begin{cases} \mathcal{H}_0 : & \mathbf{R}_n \sim \mathcal{N}(0, \boldsymbol{\Sigma}_{\mathbf{R}}), \\ \mathcal{H}_1 : & \mathbf{R}_n \sim \mathcal{N}(\mathbf{a}_n, \boldsymbol{\Sigma}_{\mathbf{R}}), \end{cases}$$

$$\boldsymbol{\Sigma}_{\mathbf{R}} = [\mathbf{I} - \mathbf{H}(\mathbf{H}^T \boldsymbol{\Sigma}_e^{-1} \mathbf{H})^{-1} \mathbf{H}^T \boldsymbol{\Sigma}_e^{-1}] \boldsymbol{\Sigma}_e$$

- Proposed scheme using a sequence of measurements that would lead to more reliable decisions.
    - conventional state estimation for false data injection detection uses only snapshot measurements in SG SE.

Multi-thread CUSUM Algorithm

- Average run length (ARL) for declaring attack:

$$T_h = \inf\{n \geq 1 | S_n > h\} \left\{ \begin{array}{l} \text{Declare the attacker is existing!} \\ \text{Otherwise, continuous to the process.} \end{array} \right.$$

- Performance Statistics:

How about the unknown?

$$S_n = \max_{1 \leq n \leq T_h} \sum_{i=n}^{T_h} \log \frac{f_1(\mathbf{R}_i|\mathbf{a}_i)}{f_0(\mathbf{R}_i)}$$

Prob. H1

Prob. H0

- A recursively cumulative S_n at time t:

$$S_n = \max\left[0, S_{n-1} + L_n\right], \quad S_0 = 0.$$

where likelihood ratio term of *m* measurements:

$$L_n = \log \frac{f_1(\mathbf{R}_n)}{f_0(\mathbf{R}_n)}$$

Elimination for the unknown

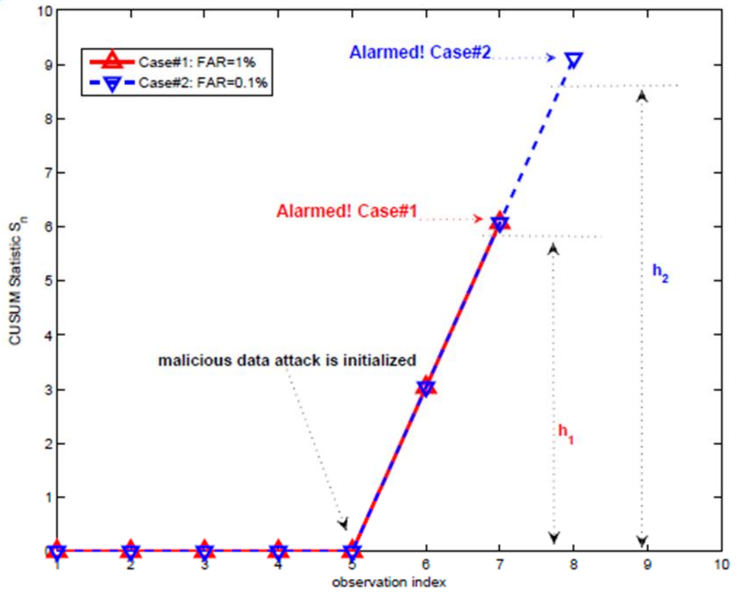
- Utilizing the properties of Rao test:
  - asymptotically equivalent model of GLRT
  - $$\mathcal{K}(\mathbf{R}_n) = \frac{\partial L_n}{\partial \mathbf{a}_n}\bigg|_{\mathbf{a}_n=\mathbf{0}}^T \left[\mathbf{J}^{-1}(\mathbf{a}_n)\bigg|_{\mathbf{a}_n=\mathbf{0}}\right] \frac{\partial L_n}{\partial \mathbf{a}_n}\bigg|_{\mathbf{a}_n=\mathbf{0}},$$
  - Equivalent necessity of inverse J^{-1} → cov. **R**
  - Quadratic formulation
- Recursive statistics after elimination:

The unknown is no long involved

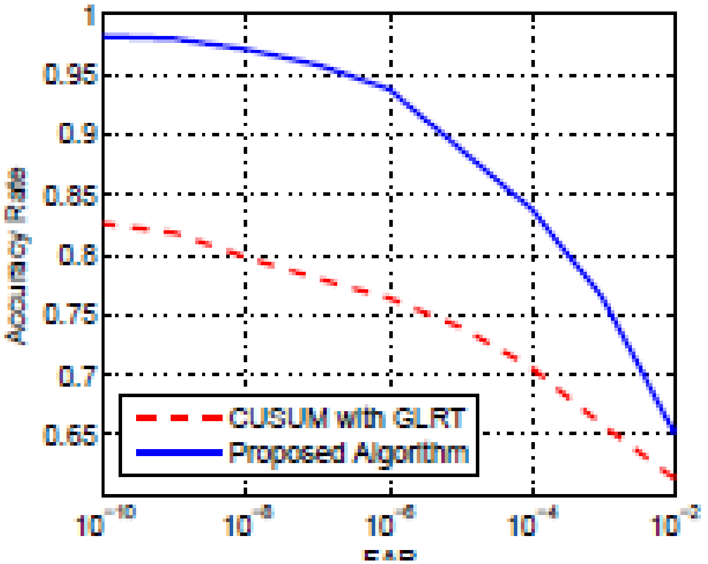
$$S_n = \max\left\{0, S_{n-1} + \mathcal{I}_n\right\}$$

where $\mathcal{I}_n = [(\mathbf{R}_n^T \Sigma_{\mathbf{R}}^{-1})^T + \Sigma_{\mathbf{R}}^{-1}\mathbf{R}_n]^T \Sigma_{\mathbf{R}} [(\mathbf{R}_n^T \Sigma_{\mathbf{R}}^{-1})^T + \Sigma_{\mathbf{R}}^{-1}\mathbf{R}_n].$

Simulation



- *Setup:* 2 α–leave detection: FAR: 1% and 0.1%, Active attack starts at 5 (randomized)
- *Result:* tradeoff btw. FAR, h, vs. detection delay

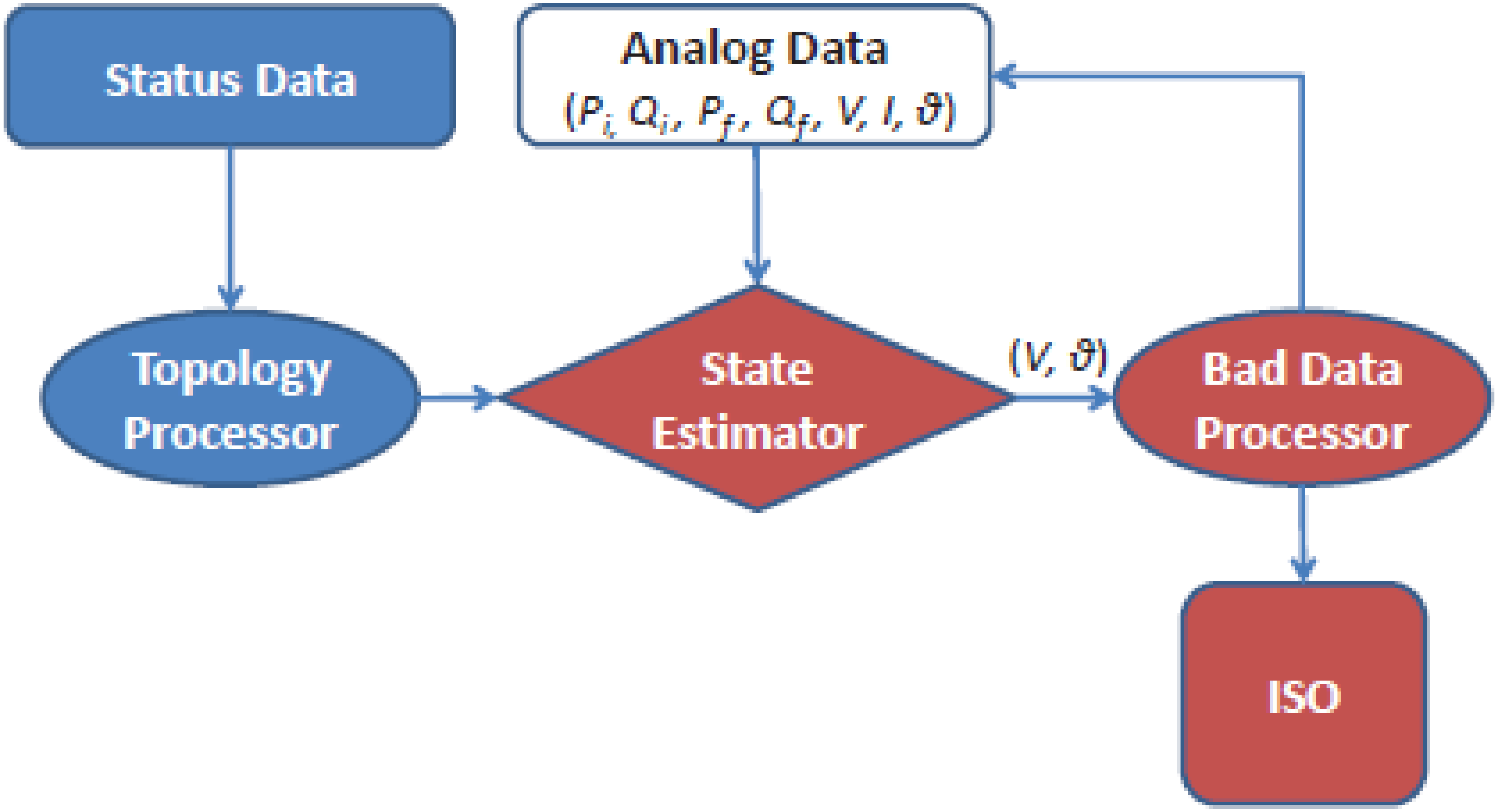


- *Setup:* 5000 realizations, 1E-10~1E-2 P_f , active attack at 6 (fixed)
- *Result:* outperform GLRT, E(T_D) 50% less
- Given extreme low P_f , successive rate is higher

Outline

- Introduction
  - What’s Smart Grid?
    - Legislations, Programs, Standards
    - Structure Overview and Challenges
  - Motivation for Quickest Detection
- Accomplishments
  - Real-Time Detection of False Data Injection in Smart Grid Networks: An Adaptive CUSUM Method and Analysis
  - **Adaptive Quickest Estimation Algorithm for Smart Grid Network Topology Error**
  - Online Quickest Multiarmed Bandit Algorithm for Distributive Renewable Energy Resources
- Summary
- Future work

Network Topology Error



Main Contributions

- Fast topology H estimation based on Z only
  - Conventional way: status data (in/out/0) at each bus sensed/collected/analyzed/send-to-SCADA, a long process
  - SG delay sensitive; a capability of responding abnormal promptly
- Reduce on vulnerability to system failure:
  - Effective and efficient to detect/identify the topology in timing manner.
  - Sequential estimation framework and considering P_{error}
- No additional cost for new hardware:
  - Avoid deployment of additional sensors, expensive hardware
- Major publication
  - Accepted, IEEE Journal on Systems: Special Issue on Smart Grid Communications

Network Topology Error

- $$\overbrace{\mathbf{Z}_n^e}^{\text{measurement}} = (\underbrace{\mathbf{H}}_{\text{topology}} + \overbrace{\mathbf{B}}^{\text{topology error matrix}})\underbrace{\mathbf{x}}_{\text{system state}} + \underbrace{\mathbf{e}_n}_{\text{noise}},$$
  - It is caused by either an branch outage, bus split, or shunt cap/reactor switching.
- The formulation of **H** is presented as the direction of power-flow:
  - e.g. Given Z_{12} , [out] (-1) for i=1, [in] (+1) for i=2 , (0) for i=3,4,…, etc

Decoding element of H @ bus *i* row *r*:

- Formulating the hypothesis:

$$\begin{cases} \mathcal{H}_0 : Z_D \sim \mathcal{N}(-\hat{x}, \sigma_D^2), \\ \mathcal{H}_1 : Z_D \sim \mathcal{N}(0, \sigma_D^2), \\ \mathcal{H}_2 : Z_D \sim \mathcal{N}(\hat{x}, \sigma_D^2), \end{cases}$$

Topology (-1) case

Topology (0) case

Topology (+1) case

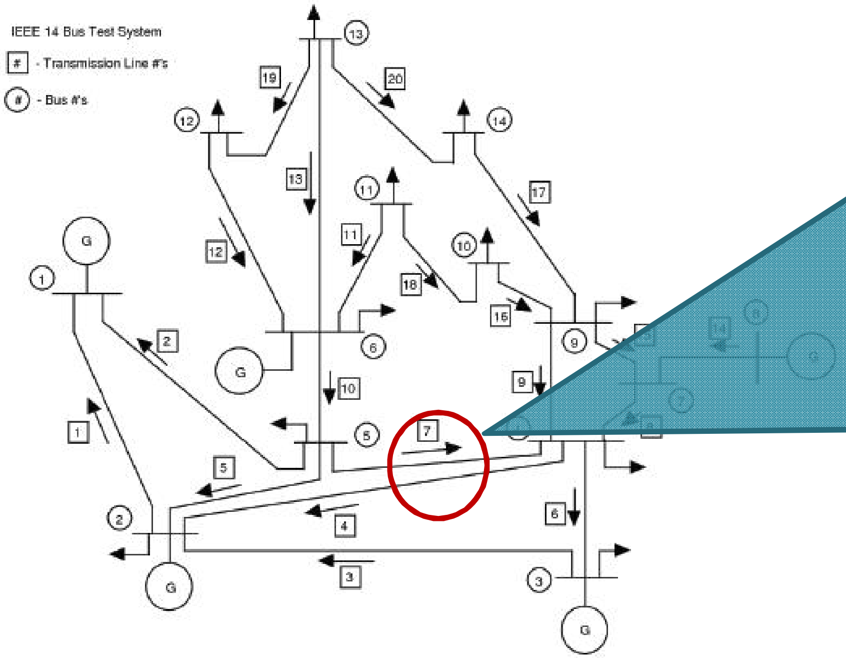
- Estimating element of H:

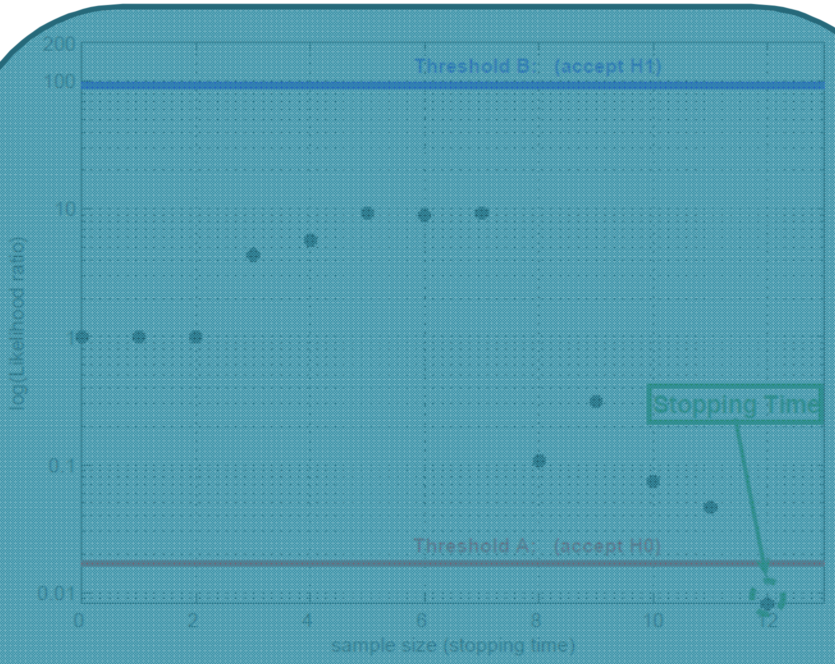
$$\hat{H}_{r,i} = \begin{cases} \textit{Test 1:} & \mathcal{H}_0 & \text{vs.} & \mathcal{H}_1, \\ \textit{Test 2:} & \mathcal{H}_1 & \text{vs.} & \mathcal{H}_2, \\ \textit{Test 3:} & \mathcal{H}_2 & \text{vs.} & \mathcal{H}_1, \end{cases}$$

3 SHTs conducts simultaneously:

- Inside of each test:
  - The minimum stopping time: $T = \inf\{k \geq 1 | \Lambda_k \ni (A, B)\},$
  - The performance measurement: $\Lambda_k = \frac{q_1(Z_k)}{q_0(Z_k)} \Lambda_{k-1}, k = 1, 2, \cdots.$
  - Upper threshold: $B = \frac{1 - \pi_0^{\pi}}{\pi_0^{\pi}} \frac{\pi_U}{1 - \pi_U}.$
  - Lower threshold: $A = \frac{1 - \pi_0^{\pi}}{\pi_0^{\pi}} \frac{\pi_L}{1 - \pi_L},$
    - Notice that π_L and π_U is determined based on cost function and prior probability.
  - Updating Likelihood ratio term til the condition satisfied
- Compare $H_{r,i}$ vs. $\hat{}H_{r,i}$ accordingly; signal when there is an error

Simulation





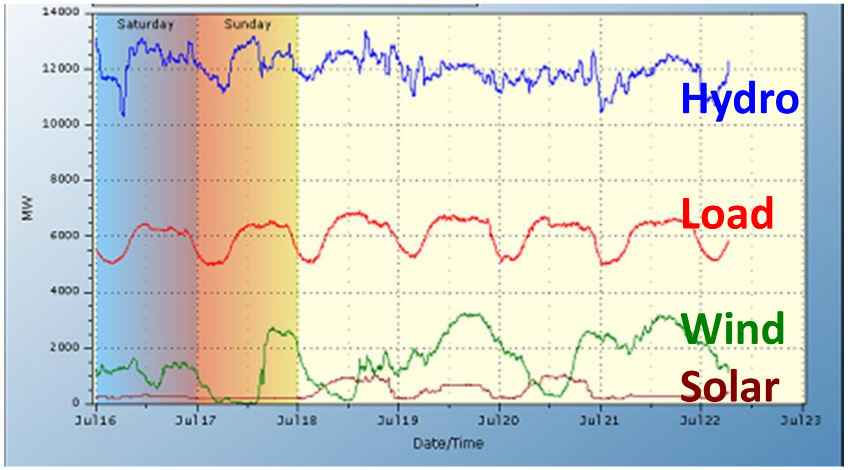
- *Setup:* MATPOWER 4 package , IEEE 14bus test system, 5 generators, 20 measurements

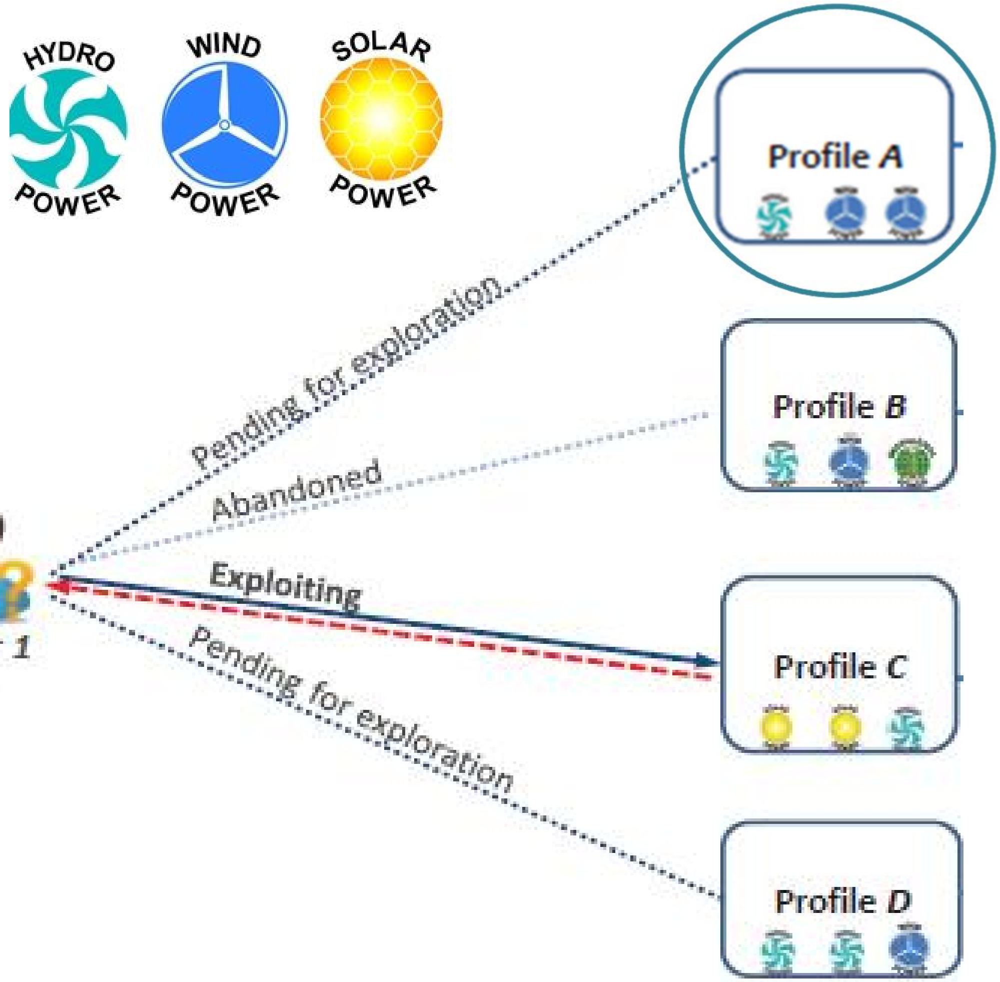
- Z_{54} , estimating $H_{r,5}$
- cumulated until it going into the region of H1 or H0, otherwise it will continues sampling. In this case, H0 is true, $H_{r,5}$ correctly determined as -1,

Outline

- Introduction
  - What’s Smart Grid?
    - Legislations, Programs, Standards
    - Structure Overview and Challenges
  - Motivation for Quickest Detection
- Accomplishments
  - Adaptive Quickest Estimation Algorithm for Smart Grid Network Topology Error
  - Real-Time Detection of False Data Injection in Smart Grid Networks: An Adaptive CUSUM Method and Analysis
  - **Online Quickest Multiarmed Bandit Algorithm for Distributive Renewable Energy Resources**
- Summary
- Future work

Illustration of System Model





How to balance among decision time, exploration, and exploitation?

Main Contributions

- Determine the best choice of long-term renewables profile in timing manner
  - Balancing btw. Decision time, exploration, and exploitation
- A online learning technique to learn evolution of renewables pattern in term of reliability
  - taking into account the uncertainty and variability of energy source
- Great potential for online strategizing allocation
  - EV scheduling, DRER allocation, etc.
- Major publication
  - Accepted, IEEE Conference on Smart Grid Communication. (Best paper award)

Preliminary

- This is an application from end-user perspective
  - It is a competitive environment
    - The utility companies unlikely publish such sensitive data;

otherwise, all consumers use the best one and the others get zero.

- System remains in steady/quasi-steady state during a short time
    - Step 1: customer applies the proposed scheme to find the best profile
    - Step 2: customer uses and trades with this profile
    - Step 3: After a certain period of time, the renewable energy distribution is changing sufficiently, and then our algorithm is triggered to find the new best profile and then trade again

Proposed Scheme

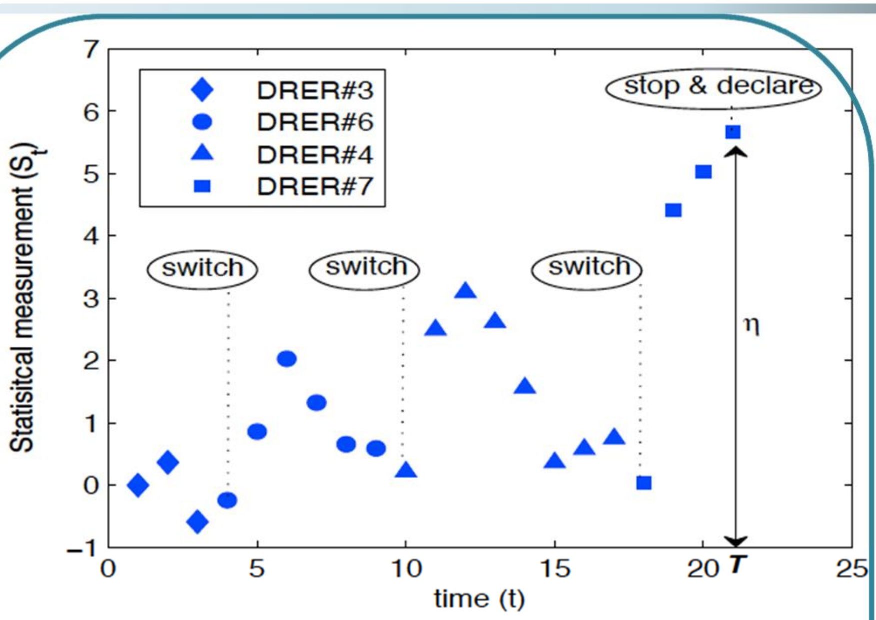
- Given a total of active K profiles
- Determine $P_{i,0}$ of each profile i at time 0
- Select a profile w/ highest $P_{i,0}$
- Repeat $t \leftarrow (1,2,3,\cdots)$
  - Cumulate $S_{i,t}$ in recursive way of $[S_{i,t-1} + L_{i,t}] + I_{i,t}$
  - Update $P_{v,t}$ with $I_{v,t}$ ($v \neq i$)
  - Switch to the profile v, if $P_{v,t} > S_{i,t}$; reset and break
- End if $S_{i,t}$ > a certain threshold
- Continues the analysis silently in case of wrong

Previous S

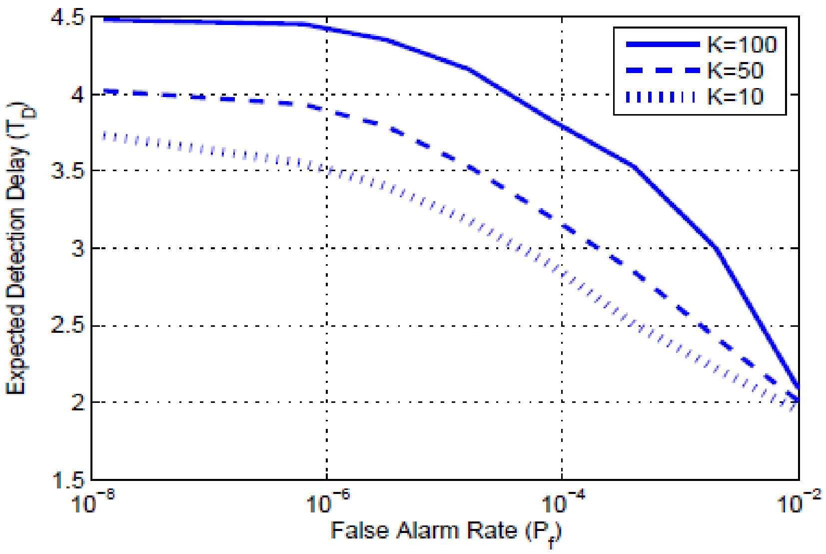
likelihood ratio P(H1)/P(H0)

Confidence interval

Performance of algorithm



- *Setup*: 10 active profiles, 0.1% P_f
    - DRER#7 has unit profit, the rest of them follows U(0,1)
- *Result*: 3 switch points, T=21, DRER#7 is selected as a long-term energy supply.



- *Setup:* 500 runs, 1E-8~1E-2% P_f , 10~100 profiles , DRER#7 has unit profit, the rest of them follows U(0.1)
- *Result:* P_f vs E(TD), K↑ T_D↑ T↑

  Gradually increased K=100

Summary

- Defensing false data injection based on CUSUM
  - A change point detection/decision algorithm
  - Low complexity approach, useful in reality.
- Identifying/locating network topology error
  - Sequential estimation framework, predefined P_{error}
  - Reduce on vulnerability to system failure
- Renewables profile allocation in term of reliability
  - Balancing btw. decision time, exploration, exploitation
  - Learning evolution of renewables profiles in term of reliability.

Publications

- Yi Huang, Jin Tang, Yu Chen, Husheng Li, Kristy A. Campbell, and Zhu Han, *“Real-time Detection of Malicious Data Injection in Smart Grid Networks: An Adaptive CUSUM Method and Analysis”*, *major revision ,* IEEE Transactions on Smart Grid: Cyber and Physical Security Systems
- Yi Huang, Mohammad Esmalifalak, Yu Chen, Husheng Li, Kristy A. Campbell, and Zhu Han, *“Adaptive Quickest Estimation Algorithm for Smart Grid Network Topology Error”,* to appear, IEEE Journal on Systems: Special Issue on Smart Grid Communication
- Yi Huang, Mohammad Esmalifalak, Huy Nguyen, Rong Zheng, Zhu Han, Husheng Li, and Lingyang Son, *“Bad Data Injection in Smart Grid: Attack and Defense Mechanisms”*, to appear, IEEE Communications Magazine: Cyber Security Smart Grid Series
- Yi Huang, Lifeng Lai, Husheng Li, Wei Chen, and Zhu Han, “Online Quickest Multiarmed Bandit Algorithm for Distributive Renewable Energy Resources”, to appear, IEEE Conference on Smart Grid Communication, 2012, [Best paper award]
- Yi Huang, Jin Tang, Yu Chen, Husheng Li, Kristy A. Campbell, and Zhu Han, *“Defending False Data Injection Attack on Smart Grid Network Using Adaptive CUSUM Test”,* IEEE Conference on Information Sciences and System, March 2011.

Future work

- CUSUM based detection in fully-distributed SG SE:
  - Communication bottleneck, reliability problems with one coordination center, interconnection btw region grid (wide area monitoring and control)
  - Design fully-distributed schemes so that each node converges almost surely to the centralized sufficient statistic.
- Optimality of sequential BDD algorithm in SG SE
  - Define an estimation performance measure and seek to the optimize it while ensuring satisfactory of the detection performance
  - Minimize the estimation-related cost subject to appropriate constraints on the tolerable levels of detection errors
- Real-world implementation and test for QD in SG
  - Acquire the real data from utilities, USRP2 to simulate SG communication
- Quickest genome scan, QD in biomedical signal monitoring, etc

Thank you for listening!