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

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 Act 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 meet the needs
- Use sophisticated comm. Technology to find/fix problems faster, enhancing reliability
- Connect grid to charge overnight when demand is low
- Gather, monitor the usage so the supply more efficiently and anticipate challenging peaks
- Can generate own and sellback excess energy

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

- Renewables fluctuant
- System complexity
- Large scale deployment
- Privacy preservation
- Complicated Decision making process
- 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 respond events promptly to help prevent catastrophic failures

Smart Grid

- Resource Management
- Network Status
- Network Security
Basic QD: Statistical Hypothesis Test

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. $t_{\text{change}}$ and $t_{\text{detect}}$
  - maintaining a certain level of detection accuracy
  - $\min [\text{processing time}], \ s.t. \ \text{Prob. error} < \eta$

* 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:**
  - Size of $Z$ >> size of $x$. (adv. of matrix redundancy)
  - Applying WLS, estimated system state $\hat{x} = (H^T \Sigma_e^{-1} H)^{-1} H^T \Sigma_e^{-1} Z_n$

- **Bad date processer computes residual:** $R_n = Z_n - \hat{Z}_n$
  - $\hat{Z}_n = H\hat{x} = H (H^T \Sigma_e^{-1} H)^{-1} H^T \Sigma_e^{-1} Z_n = \mathbb{S} Z_n$
  - $E(R_n) = 0$ 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
  \[ Z_n = Hx + b_n + e_n. \]
  where $a_n = \mathcal{G}b_n$
  Unknown mean vector $a_n$

- Using residual $R$ to forms SHT:
  \[ R_n = Z_n - \hat{Z}_n \]
  \[ \begin{cases} \mathcal{H}_0 : & R_n \sim \mathcal{N}(0, \Sigma_R), \\ \mathcal{H}_1 : & R_n \sim \mathcal{N}(a_n, \Sigma_R), \end{cases} \]
  $\Sigma_R = [I - H(H'\Sigma^{-1}_eH')^{-1}H']\Sigma_e$

- 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:
  \[ T_h = \inf\{n \geq 1 | S_n > h} \]
  Declare the attacker is existing!
  Otherwise, continuous to the process.

• Performance Statistics:
  \[ S_n = \max_{1 \leq n \leq T_h} \sum_{i=n}^{T_h} \log \frac{f_1(R_i|a_i)}{f_0(R_i)} \]

• A recursively cumulative \( S_n \) at time \( t \):
  \[ S_n = \max [0, S_{n-1} + L_n], \quad S_0 = 0. \]

  where likelihood ratio term of \( m \) measurements:
  \[ L_n = \log \frac{f_1(R_n|a_i)}{f_0(R_n)} \]
Elimination for the unknown

- Utilizing the properties of Rao test:
  - asymptotically equivalent model of GLRT
  - Equivalent necessity of inverse $J^{-1}$ cov. $R$
  - Quadratic formulation

- Recursive statistics after elimination:
  \[ S_n = \max \{ 0, S_{n-1} + \mathcal{I}_n \} \]

where
\[ \mathcal{I}_n = \left( (R_n^T \Sigma_R^{-1})^T + \Sigma_R^{-1} R_n \right)^T \Sigma_R \left( (R_n^T \Sigma_R^{-1})^T + \Sigma_R^{-1} R_n \right). \]
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

- Status Data
- Analog Data: $(P_i, Q_i, P_f, Q_f, V, I, \theta)$
- Topology Processor
- State Estimator
- Bad Data Processor
- ISO
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

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

- Estimating element of $H$:

3 SHTs conducts simultaneously:

- Inside of each test:
  - The minimum stopping time:
  - The performance measurement:
  - Upper threshold:
  - Lower threshold:

\[
B = \frac{1 - \pi_0^T}{\pi_0^T} \frac{\pi_U}{1 - \pi_U},
\]
\[
A = \frac{1 - \pi_0^L}{\pi_0^L} \frac{\pi_L}{1 - \pi_L},
\]

- Notice that $\pi_L$ and $\pi_U$ 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

Evaluation:

- $Z_{54}$, 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
  - $t \leftarrow (1, 2, 3, \ldots)$
  - 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 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 $E(T_D)$, $K \uparrow$ $T_D \uparrow$ $T \uparrow$
  - 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 $P_{\text{error}}$
  - 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


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!