Towards More Effective & Resilient Power Apps Exploiting Better Comms. & Computation

Prof. Dave Bakken

School of Electrical Engineering and Computer Science
Washington State University
Pullman, Washington, USA

NASPI Work Group Meeting
San Mateo, CA
March 24, 2015

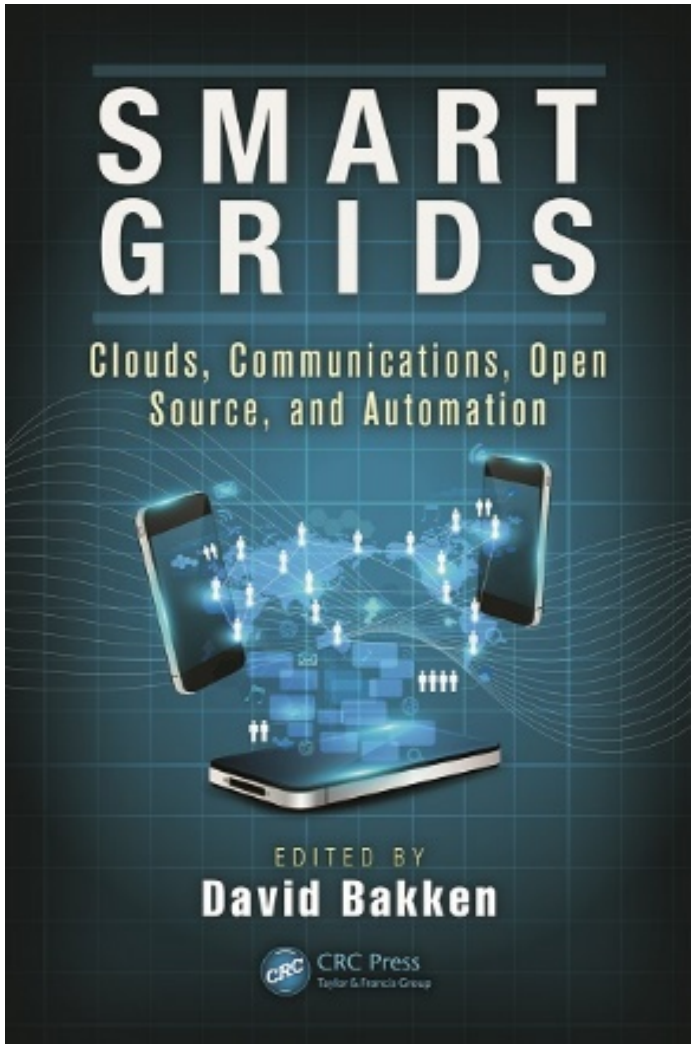
WASHINGTON STATE UNIVERSITY

The Issue

- In the last 30 years the state of the art and practice has increased a LOT in
  - Computer networking
  - Distributed computing (esp. middleware & cloud)
- The way many power researchers write their programs has not leveraged these advances
- Outline of the talk
  - Summarize what the state of the art is
  - Pose questions power researchers can ask themselves to better utilize communications and computation

Context

- IANAPP (power person): Computer Scientist
  - Core background: fault-tolerant **distributed computing**
  - Research lab experience (BBN) with wide-area middleware with QoS, resilience, security, …. for DARPA/military
  - Working with Anjan Bose since 1999 on **wide-area** data delivery issues appropriate **for RAS and closed-loop applications**
    - **GridStat (1999-present)**
    - **GridSim (2009-2014)**
    - **GridCloud (2012-present)**



May, 2014 | ISBN: 1482206110

WASHINGTON STATE UNIVERSITY

gridstat.net

Comms Baseline: You Can Assume

- Data delivery over WAN **can** be (with GridStat etc):
  - Very **fast**: less than ~1 msec added to the underlying network layers across an entire grid
  - Very **available**: think in terms of up to 5+ 9s (multiple redundant paths, each with the low latency guarantees)
    - **Even in the presence of failures!**
  - Very **cyber-secure**: for long-lived embedded devices and won't add too much to the low latencies
    - E.g., RSA adds >>60 msec so not for RAS or closed-loop
    - Shared keys (61850-90-5): subscriber can spoof publisher ☹
    - GridStat solution not vulnerable and only adds ~1msec
  - Tightly **managed** for **very strong guarantees** (~~MPLS~~)
  - **Adaptive**: can change pre-computed subscriptions ~INSTANTLY (and dynamic requests FAST)

Questions to Ask Yourself

- So how can power researchers exploit this better communications infrastructure?
- What **rate** and **latency** and **data availability** does my power app *really* need for remote data?
  - Why fundamentally does it need that?
  - How sensitive is it to occasional longer delays, periodic drops (maybe a few in a row), or data blackouts for longer periods of time?
- Can I formulate and test hypotheses for the above?

Beyond Steady-State-Only Thinking

- Previous is just for steady state: different in some contingency/mode situations?
- What extra data feeds (or higher rates etc) could I use in a contingency/mode (could get in << 1sec)
- How important is my app *in that given contingency/mode, compared to other apps?*
  - E.g., simple "importance" number [0,10]
  - How much worse QoS+ (latency, rate, availability) can I live with in steady state and in given contingencies?
    - But would **still get strong guarantees** at that lower quality
    - How much benefit do different levels really give me?
  - Can I program my app to run at different rates, or is there a fundamental reason it has to run at one?

Bad Data

- How vulnerable is my power app to bad data?
  - State estimation obviously has handed for many decades
- But
  - How much bad data
  - Does how much bad
  - In what (power) circumstances?
- E.g. can I specify assumptions about bad data?
  - Number: absolute or (better) as a function of the problem size (state/configuration/#PMUs/etc)
  - Location and timing: randomly distributed or worst case?
  - Error degree: randomly off (what probability distribution) or worst case (from an adversary)?

Bad Manners

- How vulnerable is my power app or RAS scheme or stability assumptions to worst-case malicious behavior?
- E.g. not just false data (which may be able to be detected) but taking over command of a relay or other devices
  - How many of these, and of what kind, could cause problems?
- Thinking cyber-physical here
  - What are some worst case combinations of a physical attack (rifle, chaff, modifying sensors, ..) and a cyber attack (colluding customer meters, taking over relays, DDOS to throttle delivery of sensor data and commands,
  - And worst case under what situations?

Bad Manners (cont.)

- "The event I fear most is a physical attack in a successful cyber-attack in conjunction with responders' 911 system or *on the power grid*,"
  - Ronald Dick, director of the FBI's National Infrastructure Protection Center, *Washington Post*, Front Page Article, June 27 2002, (*emphasis* added)

A Cloudy Forecast

- What could I do with cloud computing, assuming it is made mission critical, i.e.:
  - Keeps same fast throughput
  - Does not allow deliberate "inconsistencies"
    - e.g., a replica does a state update never received by others
  - Is much more predictable with CPU perf., ramp-up time, …
  - (BTW, ARPA-E GridCloud proj. w/Cornell+WSU doing for >2 years)
    - Pilot starting with ISO-New England, likely others soon
  - **Not all CPUs in datacenter, some (managed) in substations… (Cisco Fog?)**
- How could I use
  - Tens/Hundreds of processors in steady state
  - **>>Thousands when approaching/reaching contingencies**
  - Data from ALL participants in a grid enabled quickly when approaching a crisis

CIP-Managed Compute+Comms+Security

- Computations + communications + security *can* be
  - Mission critical to power grid specs
    - Closed-loop WAN app requirements **WAY harder** than air traffic control, railways, military, …
  - Changed rapidly in a coordinated manner
    - Providing app developers **much higher-level building blocks**
  - Managed in a network operations center 24x7
    - **Much like a power control center!!!**
    - Needed if power grid stability really does depend on comms and computation and cyber-security
    - No more hard-coded and unmonitored comms infrastructures causing headaches when glitches occur!

Sources of Info (1)

- D. Bakken, A. Bose, C. Hauser, D. Whitehead, and G. Zweigle. "Smart Generation and Transmission with Coherent, Real-Time Data. *Proceedings of the IEEE*, 99(6), June 2011.
- David E. Bakken, Richard E. Schantz, and Richard D. Tucker. "Smart Grid Communications: QoS Stovepipes or QoS Interoperability", in *Proceedings of Grid-Interop 2009*, GridWise Architecture Council, Denver, Colorado, November 17-19, 2009. Online http://gridstat.net/publications/TR-GS-013.pdf.
  - **Best Paper Award for "Connectivity" track**. This is the official communications/interoperability meeting for the pseudo-official "smart grid" community in the USA, namely DoE/GridWise and NIST/SmartGrid.

Sources of Info (2)

- ToSG-Workshop.org
- Chapters in D. Bakken and K. Iniewski, ed. *Smart Grids: Clouds, Communications, Open Source, and Automation,* CRC Press, May 2014, ISBN 9781482206111.
  - G. Zweigle, “Emerging Wide-Area Power Applications with Mission Critical Data Delivery Requirements”.
  - D. Bakken *et. al*. “GridStat: High Availability, Low Latency and Adaptive Sensor Data Delivery for Smart Generation and Transmission.”
  - T. Gamage *et. al*. “Power Application Possibilities with Mission Critical Cloud Computing.”