Report on NSF Cyber Trust Program, Relevance to Power Systems, Secure Middleware R&D

David Bakken & Anjan Bose

Washington State University
Pullman, Washington USA

http://gridstat.net

EIPP Meeting
October 13, 2005

GridStat Overview

- Next-generation communications infrastructure for the electric power grid (Carl Hauser at EIPP Meeting in April)
  - Enabling better control and protection
  - Researching since 1999, first demo in 2002, Avista tech. demo
- Provides flexible delivery of status data, including PMUs
- "Status Routers" forward status updates and alerts with quality of service mechanisms (rate filtering, multicast)
  - SW latency ~0.5ms (Java) and 50K/sec; network processor faster
- Managed infrastructure allowing for changing status delivery and adding new subscribers with software
  - Manages multiple redundant paths for fault-tolerance
- Deployable on top of IP, ATM, network processors, …
- Funding: NIST (w/SEL), NSF (project w/CMU, center…)
- Collab. w/ Kevin Tomsovic, Mani Venkatasubramanian, …

GridStat and EIPP are Complimentary

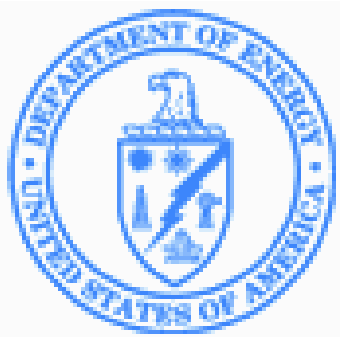
- GridStat status router forwarding mechanisms can preserve PMU synchronization in rate filtering (and multicast)
- Data Management lives at the "edges" of GridStat
  - GridStat can plug into different standards for data formats, etc.
  - GridStat allows use of GPS or other publisher-supplied timestamps
  - GridStat can be tailored to use different naming schemes for data
- Real-Time
  - Status Routers can be more configurable version of Phasor Data Concentrator (PDC)'s collection functionality
  - GridStat "condensation functions" (plugins) could do additional PDC-like correlation (or leave to end-application)
- GridStat technology squarely in "Data Communications" proposed EIPP WG
  - Much more involved than just "plugging in a network"
  - Consider Bakken & Hauser resources for wide-area QoS/networks

Reality Check

Greater flexibility in communications requires cyber security to be iron clad!

National Science Foundation Center

- Recently Announced: NSF Cyber Trust Center-Scale Award: Trustworthy Cyber Infrastructure for the Power Grid (TCIP).
  - Cyber Trust is NSF's main security research program
  - Only 4 center-scale awards have been done in history of program
    - Other one this year: electronic voting
- Funding:
  - NSF (both computer science and engineering)
  - DHS
  - DoE



TCIP Team

- Fundamentally a computer science award, with strong power engineering partnerships
  - Power researchers: Anjan Bose, Pete Sauer, Bob Thomas, George Gross, Tom Overbye
  - Industrial Advisory Board: ABB, Areva, Cisco, Honeywell, TVA, Entergy, GE, Cal ISO, …
    - Education, outreach, and tech transfer is a key TCIP goal
- Partner universities
  - University of Illinois (lead)
  - Cornell
  - Dartmouth
  - Washington State University

Technical Overview

- Goal: provide the fundamental science and technology needed to create cyber infrastructure for
  - an intelligent, adaptive power grid that can
  - survive malicious adversaries,
  - provide continuous delivery of power,
  - and support dynamically varying trust/securuity requirements.
- Approach: Creating the necessary cyber building blocks and architecture, and by creating validation technology to quantify the amount of trust provided by the new mechanisms
- Researchers involved (~15) and grad students from varying backgrounds: cyber security, networking, wide-area communications software (middleware), modeling, simulation, validation, ….

Four Technical Areas

1. **Secure and Reliable Computing Base**: cybersecurity of low-level devices and their communications.
   - Sheer number of devices to be secured
   - Cost of securing them
   - Performance impacts of security on the devices' functionality
2. **Trustworthy infrastructure for data collection and control**: efficient, timely and secure measurement and aggregation mechanisms for edge device data.
   - Challenge: devising and implementing adaptable policies and mechanisms for trading off performance and security during
     - Normal conditions
     - Cyber-attacks
     - Power emergencies

Four Technical Areas (cont.)

3. **Wide-area Trustworthy Information Exchange**:
   - Mechanisms for scalable inter-domain authorization
   - Fundamental principles for security in emergency situations.
   - Approaches
     - Dynamic negotiation under normal, attack and emergency conditions
     - Mechanisms to exploit the trusted computing base.
4. **Quantitative Evaluation**: validate the TCIP designs and implementations produced in the other areas.
   - create security metrics, multi-scale abstractions and attack models
   - emulation technology to allow quantitative analysis of real power grid scenarios.

Outreach is also key: advisory board, creating new annual symposium on Cyber Trust for Power Systems

For More Information

- www.gridstat.net
- www.iti.uiuc.edu/TCIP.html
- Carl Hauser, David Bakken, and Anjan Bose. "A Failure to Communicate: Next-Generation Communication Requirements, Technologies, and Architecture for the Electric Power Grid", *IEEE Power and Energy*, 3(2), March/April, 2005, 47–55. Available for research purposes at http://gridstat.net/GridStat-Power-Energy-March05.pdf
- bakken@eecs.wsu.edu