Algorithmic Decision Theory and the Smart Grid

Fred Roberts
Rutgers University

CCICADA
Command, Control, and Interoperability Center for Advanced Data Analysis
A Department of Homeland Security Center of Excellence

DIMACS
Center for Discrete Mathematics & Theoretical Computer Science
Founded as a National Science Foundation Science and Technology Center

Algorithmic Decision Theory

- Today's decision makers in fields ranging from engineering to medicine to homeland security have available to them:
  - Remarkable new technologies
  - Huge amounts of information
  - Ability to share information at unprecedented speeds and quantities

Algorithmic Decision Theory

- **These tools and resources will enable better decisions if we can surmount concomitant challenges:**
  - The massive amounts of data available are often incomplete or unreliable or distributed and there is great uncertainty in them

Algorithmic Decision Theory

•These tools and resources will enable better decisions if we can surmount concomitant challenges:

–Interoperating/distributed decision makers and decision-making devices need to be coordinated

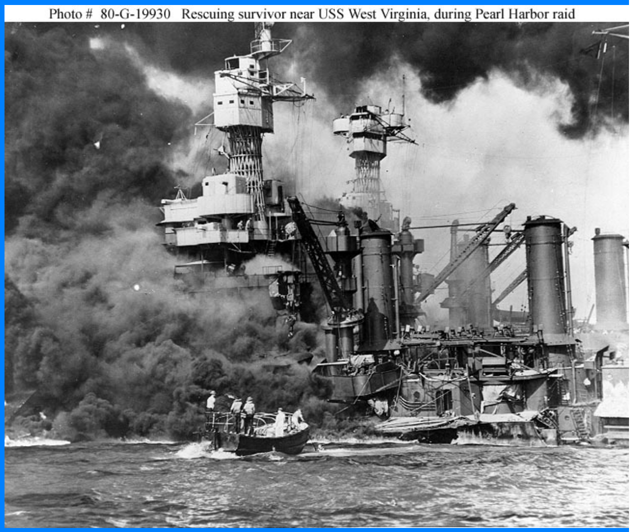
–Many sources of data need to be fused into a good decision, often in a remarkably short time

Algorithmic Decision Theory

- **These tools and resources will enable better decisions if we can surmount concomitant challenges:**
  - Decisions must be made in dynamic environments based on partial information
  - There is heightened risk due to extreme consequences of poor decisions
  - Decision makers must understand complex, multi-disciplinary problems

Algorithmic Decision Theory

- In the face of these new opportunities and challenges, ADT aims to exploit algorithmic methods to improve the performance of decision makers (human or automated).
- Long tradition of algorithmic methods in logistics and planning dating at least to World War II.
- But: algorithms to speed up and improve real-time decision making are much less common



Pearl Harbor

Algorithmic Decision Theory

- The goal of the field of ADT is to explore and develop algorithmic approaches to decision problems arising from a variety of application areas.
- This requires collaborations:
  - Computer scientists with decision theorists
  - Statisticians with economists
  - Mathematicians with behavioral scientists
  - Operations researchers with public health professionals

Algorithmic Decision Theory

- First International Conference on ADT, Venice 2009.
- Second International Conference on ADT, DIMACS Center, Rutgers University, October 2011.
- Third International Conference on ADT – Brussels, Nov. 2013
- Fourth International Conference – Lexington, KY, Fall 2015

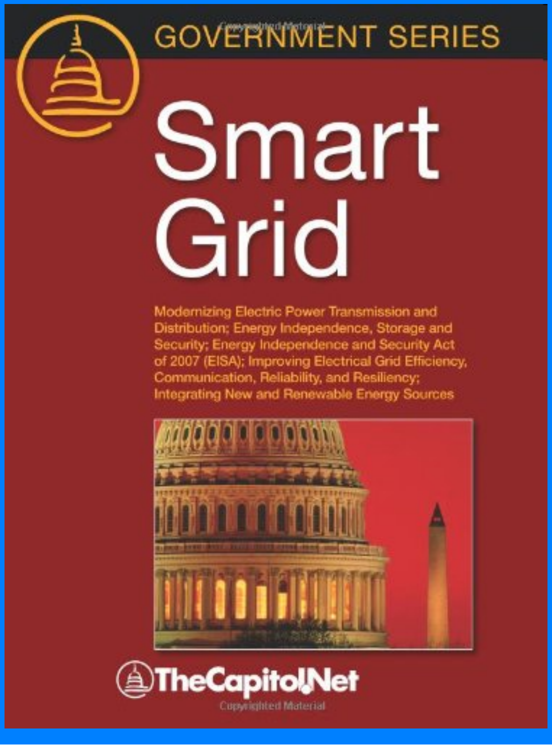
DIMACS

Center for Discrete Mathematics & Theoretical Computer Science
Founded as a National Science Foundation Science and Technology Center

ADT and Smart Grid

•Many of the following ideas are borrowed from a presentation by Gil Bindewald of the Dept. of Energy to the SIAM Science Policy Committee, October 2009.

•Others benefit from a presentation by Massoud Amin at DIMACS workshop on ADT and the Smart Grid, October 2010.



Today's Electric Power Grid

- Today's electric power systems have grown up incrementally and haphazardly – they were not designed from scratch
- They form ***complex systems*** that are in constant change:
  - Loads change
  - Breakers go out
  - There are unexpected disturbances
  - They are at the mercy of uncontrollable influences such as weather

Today's Electric Power Grid

•Today's electric power systems operate under considerable uncertainty
•Cascading failures can have dramatic consequences.

Today's Electric Power Grid

- **Challenges include:**
  - Huge number of customers, uncontrolled demand
  - Changing supply mix system not designed for complexity of the grid
  - Operating close to the edge and thus vulnerable to failures

Today's Electric Power Grid

- **Challenges include:**
  - –Interdependencies of electrical systems create vulnerabilities
  - –Managed through large parallel computers/ supercomputers with the system not set up for this type of management

The Blackout of 2003

- ***Basic Message: Increasing the complexity of a system can have unintended consequences***

- Aug. 14, 2003: Shortly after noon, a 375 megawatt generating plant in central Ohio went offline
- An hour later, a 785 megawatt plant north of Detroit went offline, followed by a large plant in northern Ohio.

Acknowledgement: Article by Sara Robinson, SIAM News, Oct. 2003

The Blackout of 2003

• ***Basic Message: Increasing the complexity of a system can have unintended consequences***

•Then at 2 PM a brush fire forced a high-voltage transmission line carrying many megawatts of power from southwest Ohio to northern Ohio to disconnect itself.

Acknowledgement: Article by Sara Robinson, SIAM News, Oct. 2003

The Blackout of 2003

- Electricity coursing through the grid “seamlessly” adjusted to the losses, rerouting itself through the network – in accordance with the laws of physics.

S = P + jQ

$$\sum Pi = \text{PGenerator} + \text{PLoad} + \text{PCompensation}$$

$$\sum Qi = \text{QGenerator} + \text{QLoad} + \text{QCompensation}$$

Real Power: $P = \frac{V^2}{X} \bullet \sin\delta$

Reactive Power: $Q \approx V \bullet I \bullet \sin(\delta / 2) = \frac{V^2}{X} \bullet (1 - \cos\delta)$

V voltage
X reactance
δ phase angle
I current

- The large losses were invisible to consumers.

Acknowledgement: Article by Sara Robinson, SIAM News, Oct. 2003
Equations from Massoud Amin

The Blackout of 2003

•Meanwhile, human operators were also attempting to stabilize the system.

Acknowledgement: Article by Sara Robinson, SIAM News, Oct. 2003

The Blackout of 2003

- Operators cannot direct the flow of power along a particular pathway, but they can make adjustments that influence power flows indirectly – using computer programs to measure the state of the system and stepping up generators or shutting down lines.
- But those human decisions require lots of information and a newly implemented system in the Midwest gave the operators limited information about the state of the network.

Acknowledgement: Article by Sara Robinson, SIAM News, Oct. 2003

The Blackout of 2003

•When three more high voltage lines in Ohio overloaded and went down, the system began to lose the ability to stabilize itself.

•Ultimately, a large chunk of Canada and the United States went dark.


ROCHESTER
Democrat and Chronicle

Huge power failures
Parts of eight states and Canada left dark; cause remains in dispute.
Story below

Six pages of coverage
A roundup of blackout stories from around the region and nation.
Pages 10A-15A

No delays for PGA
Today's second round of the PG Championship will not be affect
Story below

BLACKOUT

As the blackout rolled across vast portions of the northeastern United States and southeastern Canada, officials estimated that it affected as many as 50 million people. Gov. George Pataki said

BLACKOUT, PAGE 10A

Emergency declared in Monroe, Livingston

Affected cities across the Northeast
Shortly after 4 p.m. power outages spread across the northeastern United States and parts of Ontario, Canada.
Some parts of these states or provinces were affected.

Acknowledgement: Article by Sara Robinson, SIAM News, Oct. 2003

The Need for a Smart Grid

- This kind of event is one of the motivations for a smart grid.

The Need for a Smart Grid

•Massoud Amin defines the "smart grid" this way:

The term "smart grid" refers to the use of computer, communication, sensing and control technology which operates in parallel with an electric power grid for the purpose of enhancing the reliability of electric power delivery, minimizing the cost of electric energy to consumers, improving security, quality, resilience, robustness, and facilitating the interconnection of new generating sources to the grid.

The Need for a Smart Grid

Why do we need a smart grid?

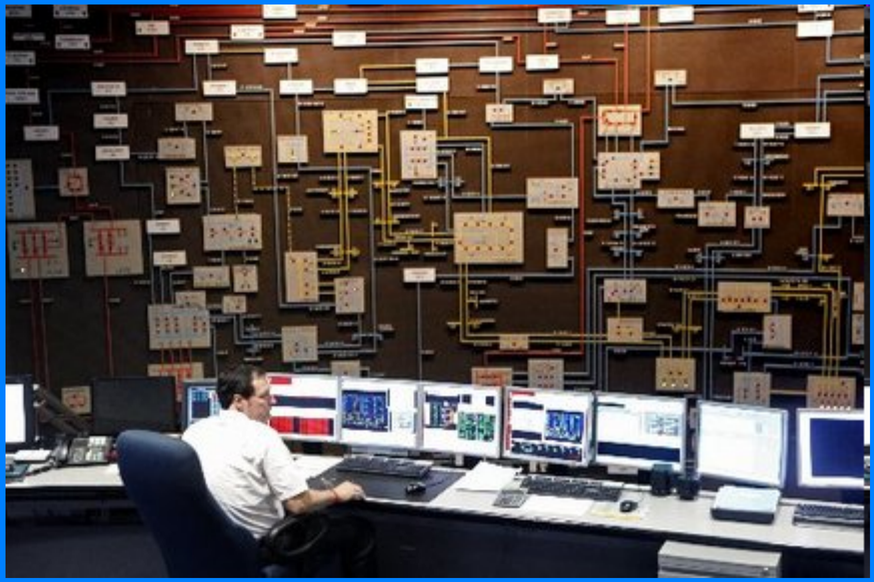
- The electric power grid is a massive, complex system.
- With sufficient information to determine what is happening in real time, grid operators would be able to contain a cascading outage or perhaps prevent one altogether.
- However:
  - –The grid has hundreds of thousands of miles of transmission lines
  - –Decisions have to be made really fast – in real time or faster

Acknowledgement: Article by Sara Robinson, SIAM News, Oct. 2003

The Need for a Smart Grid

Why do we need a smart grid?

- Power grid operators need to see several moves ahead, sorting through millions of possible scenarios, to choose an appropriate response.



Acknowledgement: Article by Sara Robinson, SIAM News, Oct. 2003

The Need for a Smart Grid

Why do we need a smart grid?

- It could be that humans just can't respond that quickly or calculate that fast.
- Either we give them some tools to aid them or we put the decision making into the hands of machines.
- This calls for the tools of algorithmic decision theory.
- What is called for is a new complex, adaptive system that has self-healing properties.

Acknowledgement: Article by Sara Robinson, SIAM News, Oct. 2003

The Need for a Smart Grid

•This idea of a "***self healing grid***" was initiated in 1998 in an EPRI/DOD initiative called the "Complex/Interactive Networks/Systems Initiative

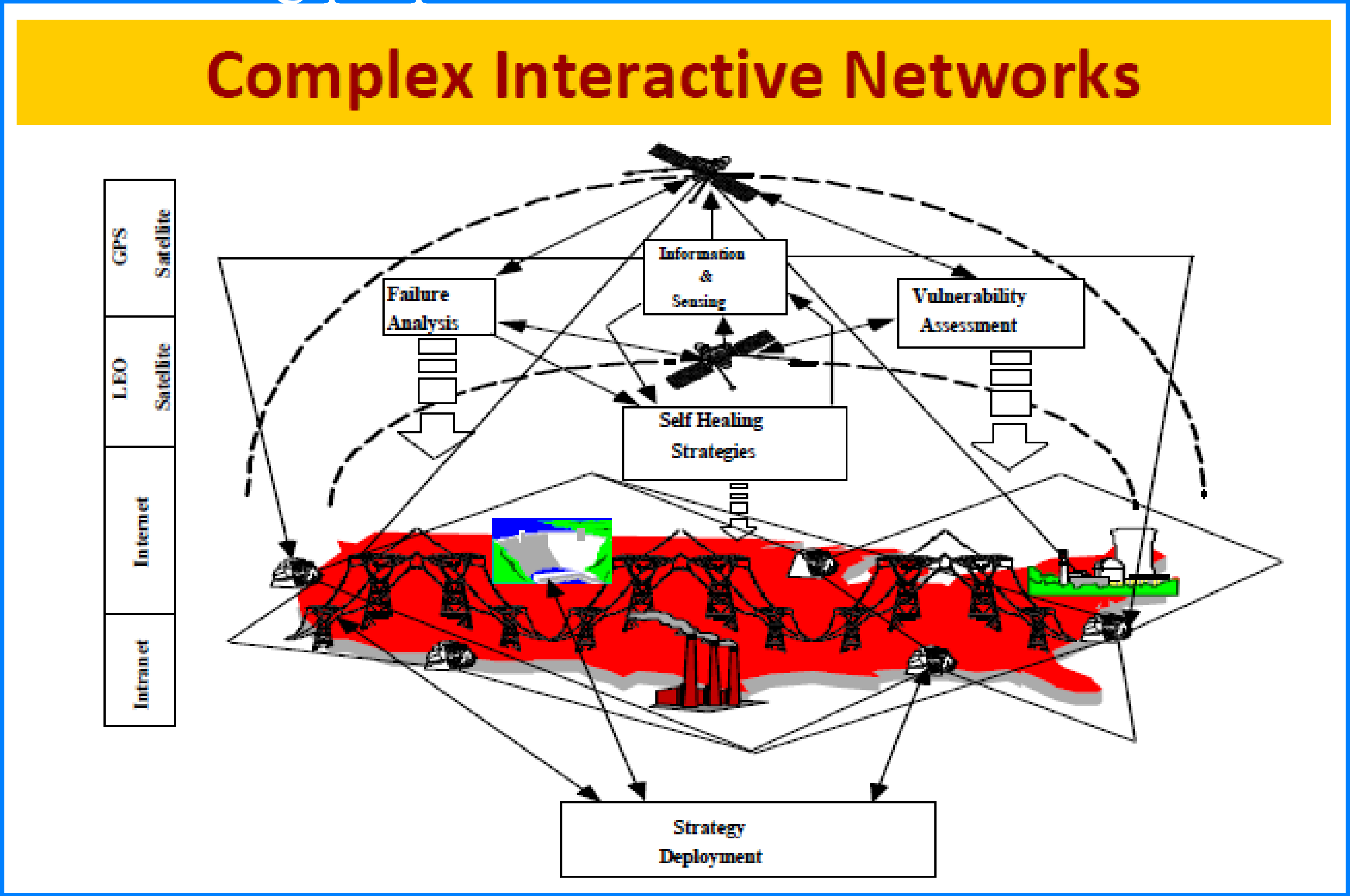
• CIN/SI funded 108 professors and over 240 graduate students in 28 U.S. universities between 1998 and 2002.

•In 2001 EPRI introduced the term "Intelligrid"

•Since then, EPRI and DOE have adopted the term "smart grid."

The Need for a Smart Grid

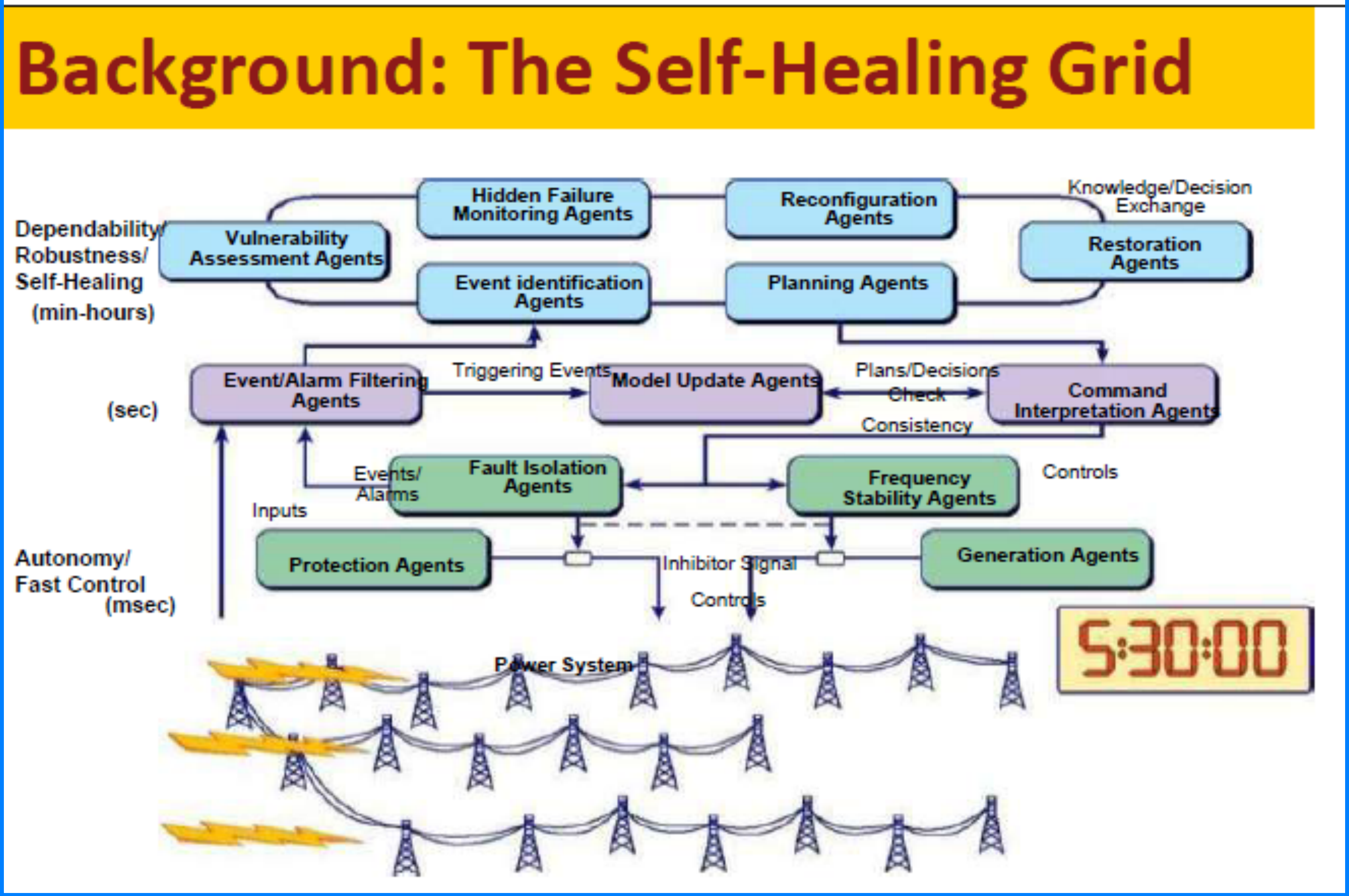
•What is called for is a new complex, adaptive system that has self-healing properties.



Credit: Massoud Amin

The Need for a Smart Grid

•What is called for is a new complex, adaptive system that has self-healing properties.



Credit: Massoud Amin

Autonomic Computing

•"Self-healing, complex adaptive system" is a concept that was generalized in the early 2000's through the notion of "***autonomic computing***," popularized by IBM.

•The goal of autonomic computing is to create computer systems that manage themselves with "high level" guidance from humans.

•Per IBM:

"Civilization advances by extending the number of important operations which we can perform without thinking about them." - Alfred North Whitehead

Autonomic Computing

Computing Research Association Grand Research Challenges for Information Systems:

- Large-scale systems have become too difficult for humans to configure, maintain and tune and too difficult for us to predict their behavior.
- The challenge is to make them self-sustaining.

Autonomic Computing

Computing Research Association Grand Research Challenges for Information Systems:

•***Self-configuration***: How do we get large-scale systems to configure themselves automatically in accordance with high-level policies that specify desired outcomes?

•***Self-optimization***: How do we get complex computing/information systems to monitor, experiment with, and modify their own parameters in order to optimize their performance and interaction with other systems?

Autonomic Computing

Computing Research Association Grand Research Challenges for Information Systems:

•***Self-maintenance***: In an environment of changing workloads, demands, and external conditions, how do we get systems to maintain and adjust their operation?

•***Self-healing, self-protecting***: How do we design complex systems to automatically discover and correct faults?

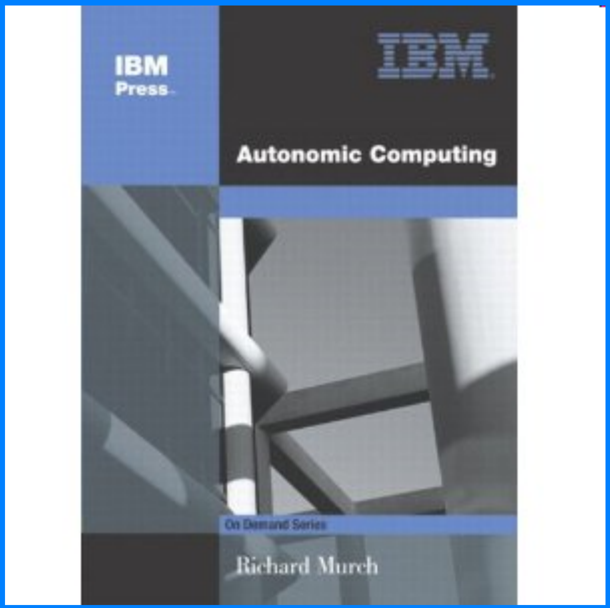
Autonomic Computing

Computing Research Association Grand Research Challenges for Information Systems:

•***Self-differentiation***: How do we design complex systems with fewer parts that have predetermined behavior and have ways to develop different behavior from similar parts?

Autonomic Computing

- Issues of autonomic computing are broader than the types of issues we encounter for smart grids.
- But certainly the self-healing, self-protecting property is a key component of the smart grid.

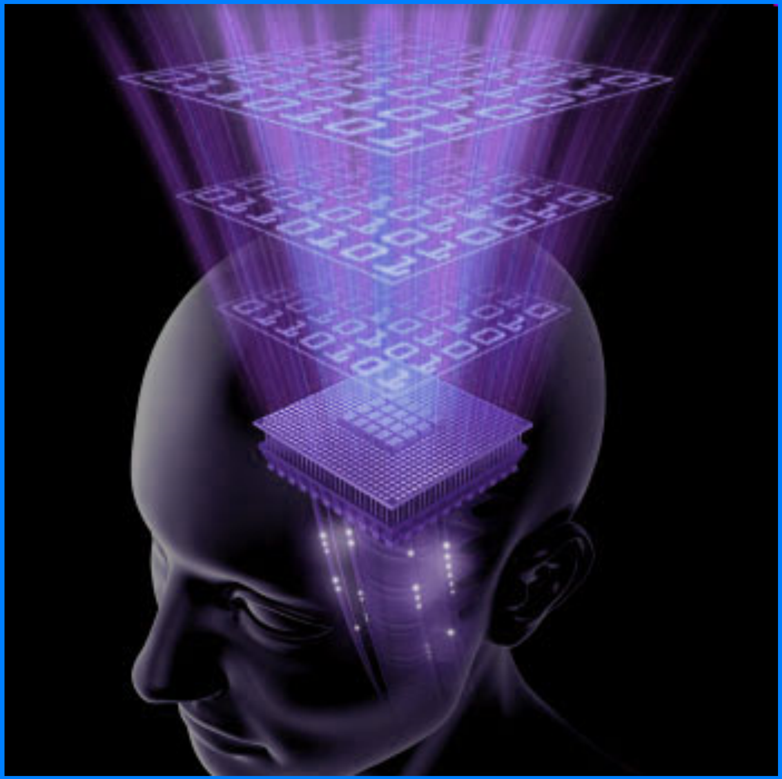


Self-Healing System Challenges

- ***Such systems will have to deal with the entire problem lifecycle:***
  - Monitoring
  - Detecting that something may be or may become broken or damaged
  - Impact analysis
  - Severity classification and notification
  - Remediation (repairing, rebooting, or otherwise working around the problem)
  - Recording problem and corrective action (for learning purposes)

Smart Grid Applications

- ***"Smart grid" applications are grounded in massive amounts of data that will enable better decisions.***



Smart Grid Applications

- **"Smart grid" data sources enable real-time precision in operations and control previously unobtainable:**
  - Time-synchronous phasor data, linked with advanced computation and visualization, will enable advances in

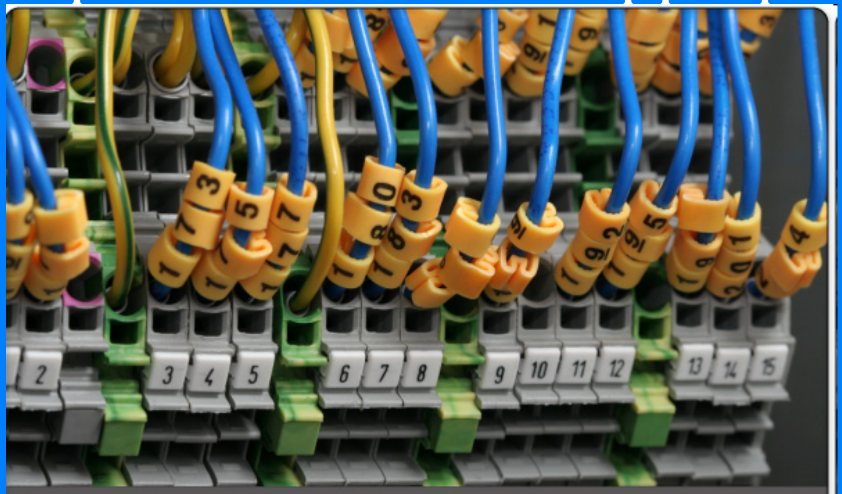
    - state estimation
    - real-time contingency analysis
    - real-time monitoring of dynamic (oscillatory) behaviors in the system

Smart Grid Applications

- **"Smart grid" data sources enable real-time precision in operations and control previously unobtainable:**
  - Enhanced operational intelligence
  - Integrating communications, connecting components for real-time information and control

Smart Grid Applications

- **"Smart grid" data sources enable real-time precision in operations and control previously unobtainable:**
  - –Sensing and measurement technologies will support faster and more accurate response, e.g., remote monitoring
  - –Advanced control methods will enable rapid diagnosis and precise solutions appropriate to an "event"


FleetZOOM Remote Annunciator Panel Monitoring

Smart Grid Applications

- **Phasor measurements** will provide "MRI quality" visibility of the power system.
- **Traditional SCADA (Supervisory Control & Data Acquisition) measurement** provides
  - Bus voltages
  - Line, generator, and transformer flows
  - Breaker Status
  - ***Measurement every 2 to 4 seconds***

Smart Grid Applications

•Phasor technology and phasor measurements provide additional data:

- –Voltage and current phase angles
- –Frequency rate of change
- –***Measurements taken many times a second***
- –This gives dynamic visibility into power system behavior

Smart Grid Applications

- **Some phasor applications:**
  - –Monitoring
    - ➢Visibility beyond local controls
    - ➢Frequency instability detection
    - ➢Triangulation to estimate location of generator dip or hard drop

Smart Grid Applications

- **Some phasor applications:**
  - Analysis/Assessment: improved state estimation
  - Planning
    - Dynamic model validation
    - Forensic analysis (figuring out what went wrong) through time tagging and synchronization of measurements
  - Protection and control: automatic arming of remedial action schemes

Smart Grid Applications

- "Smart grid" data sources enable real-time precision in operations and control previously unobtainable:
  - –Real-time data from smart meter systems will enable customer engagement through demand response, efficiency, etc.

Smart Grid Applications

- **Phasor technology and phasor measurements provide additional data:**
  - Such measurements will allow rapid understanding of how customers are using electricity.
  - This can provide them with guidance for how to conserve energy.

Smart Grid Applications

- An example of an area where smart grid applications have already paid off is in ***commercial buildings.***
- But, there are complex challenges:
  - –Energy used for overhead lighting and HVAC must be balanced with energy needed for activities
  - –Control schedules must be balanced with understanding of weather conditions and expected building occupancy

Acknowledgement: commercial building examples from Tariq Samad

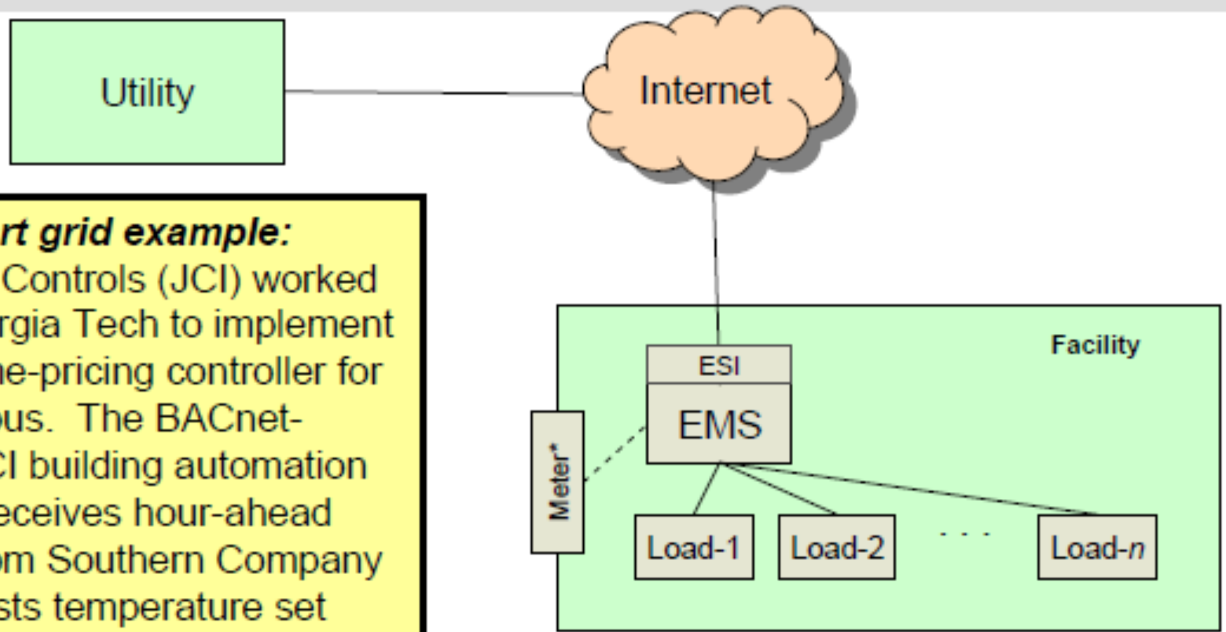
Smart Grid Applications

- An example of an area where smart grid applications have already paid off is in ***commercial buildings.***
- But, there are complex challenges:
  - Startup must be managed – electrical spikes cannot be tolerated
  - Use of thermal/ice storage (to be explained soon) can utilize knowledge of current/future cost of energy, weather information, current and future demand, existing storage capacity

Acknowledgement: commercial building examples from Tariq Samad (Honeywell)

Smart Grid Applications

Commercial smart grid information architecture (1)



*may be shadow/interval meter

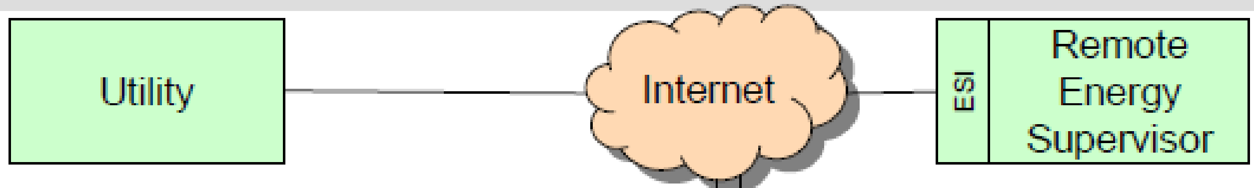
C&I smart grid example:
Johnson Controls (JCI) worked with Georgia Tech to implement a real-time-pricing controller for the campus. The BACnet-based JCI building automation system receives hour-ahead prices from Southern Company and adjusts temperature set points and boiler fuel source. Annual savings are estimated at $650K – $1M.

Courtesy of D. Alexander, Georgia Tech
For more information: http://www.fire.nist.gov/bfrlpubs/build07/PDF/b07028.pdf

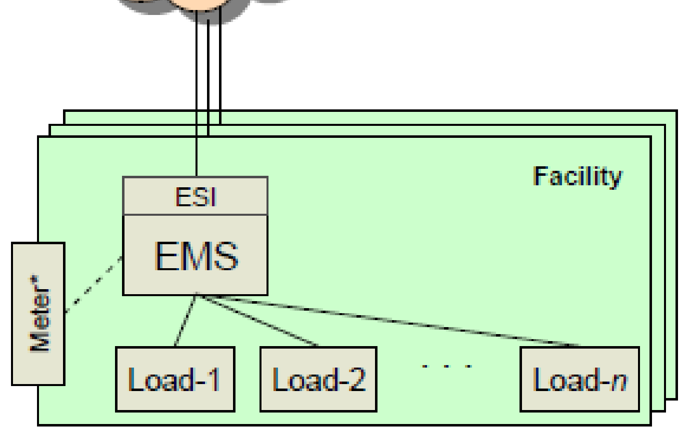
Acknowledgement: commercial building examples from Tariq Samad

Smart Grid Applications

Commercial smart grid information architecture (2)



C&I smart grid example:
Honeywell Novar is the global leader in multisite energy management, with remote energy supervision of > 10,000 sites, including 65% of the top U.S. retailers (Walmart, Home Depot, Staples, Sam's Club, ...). In the U.S., Novar manages over 6 GW of loads in commercial buildings.



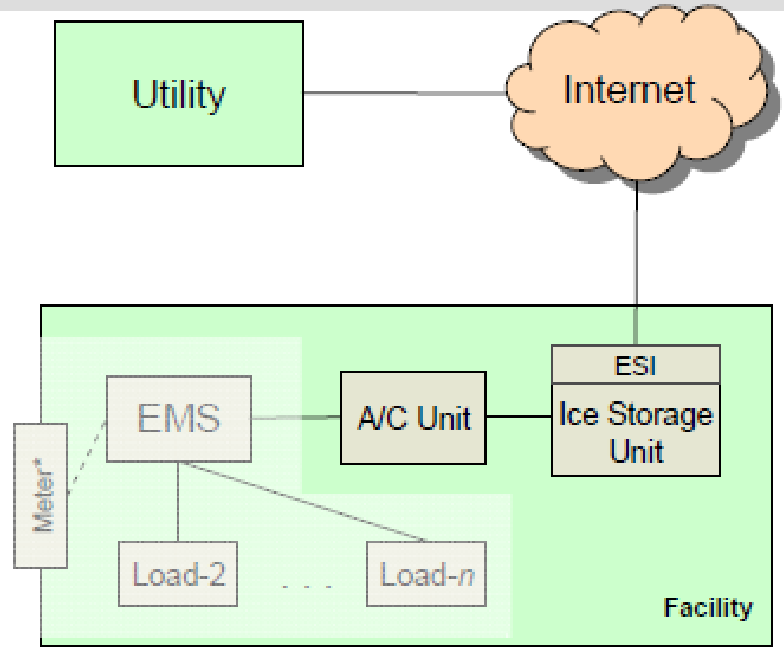
For more information: http://www.novar.com/

Acknowledgement: commercial building examples from Tariq Samad

Smart Grid Applications

Commercial smart grid information architecture (3)

C&I smart grid example:
Ice Energy's storage solution (Ice Bear) enables peak load reduction in commercial buildings through the generation of ice during off-peak times and the use of the ice for cooling during peak load. A controller and ESI are part of the Ice Bear product, which determines the energy source (the EMS controls the cooling demand). Condensing unit peak reduction of 94 – 98 per cent is routinely realized in commercial installations.



Courtesy of B. Parsonnet, Ice Energy
For more information: http://www.ice-energy.com/

Acknowledgement: commercial building examples from Tariq Samad

Smart Grid Vulnerabilities

•Physical Vulnerability: Over 215,000 miles of 230 kV or higher transmission lines and many thousand more of lower voltage lines

•Transformers, line reactors, series capacitators are also vulnerable.

Smart Grid Vulnerabilities

•Natural disasters or a well-organized group of terrorists can take out portions of the grid as they have done in the U.S., Colombia, etc.

–Open source data: Analysts have estimated that public sources could be used to obtain at least 80% of the information needed to plot an attack.

•Dependence on Information Technology: Because of the vulnerability of Internet communications, power system command, control and communication system is vulnerable

Smart Grid Vulnerabilities

- Security of new software is a priority
- Cyber attacks on the electric power grid are a major concern. Needed are methods for
  - Prevention
  - Response
  - Recovery

Smart Grid Vulnerabilities

•Cybersecurity is a major area of research at DIMACS and CCICADA and elsewhere in the homeland security community.

DIMACS

Center for Discrete Mathematics & Theoretical Computer Science
Founded as a National Science Foundation Science and Technology Center

CCICADA

Command, Control, and Interoperability Center for Advanced Data Analysis

A Department of Homeland Security Center of Excellence

Smart Grid Vulnerabilities

- Cyber attacks are a national security concern and have been increasing in frequency and sophistication over several years.
- According to a May 2010 survey by the Center for Strategic and International Studies, 59 percent of 600 IT managers operating critical infrastructure in 14 countries reported infiltrations by "high-level adversaries such as organized crime, terrorists, or nation states."

Smart Grid Vulnerabilities

- "Cyberspace" is
  - Insecure
  - Faced with attacks by adversaries who wish to take advantage of our dependence on it
- Use of cyberspace subjects us to:
  - Loss of information
  - Loss of money
  - Disruption, destruction, or interruption of critical services

Smart Grid Vulnerabilities

- A cyber attack could cripple our power supply, causing not only power failures in homes, but making it impossible for major utilities such as water to operate, stalling mass transit, and endangering the safety of many people.
- It could also impede homeland security personnel from being able to respond, react to, and address the emerging crises.

Smart Grid Vulnerabilities

- Example in Poland illustrates the ease and arrant means by which the system may be exploited.
- In 2008 a 14 year-old schoolboy was able to hack into the communications system and manipulate the tram system as if it was "a giant train set."
- The teenager converted the television control into a device, which could control all the junctions along the operating line and maneuver the trams.

Smart Grid Vulnerabilities

•Four trams derailed and twelve people were hospitalized as a result of his actions.

Smart Grid Vulnerabilities

- Our cities are critically dependent on our commuter train systems.
- Yet, a cyber attack on the signaling system could bring our commuter train traffic to a grinding halt or, worse, cause horrific train accidents.

Smart Grid Vulnerabilities

- Our discussions with railroad officials suggest that their greatest concern with respect to vulnerabilities of the rail system is attacks against command and control systems such as their SCADA systems.
- Similar concerns should apply to the smart grid.

Super Bowl 47, New Orleans

- Was it terrorism?
- Was it cyber-terrorism?
- (Luckily just a relay device failing at Entergy New Orleans)

Credit: businessinsider.com

Super Bowl 48, New Jersey

Credit: new.mta.info

NJ State Police Regional Operations Intelligence Center assessment:

- ***Cyber attacks by "ideologically motivated and malicious" hackers, exploiting wireless systems, on stadium infrastructure or Super Bowl websites, is a serious possibility.***

CCICADA Project: Best Practices for Stadium Security & Analyses of Security Processes

Supported by DHS Office of SAFETY Act Implementation

CCICADA
Command, Control, and Interoperability Center for Advanced Data Analysis
A Department of Homeland Security Center of Excellence

Lambeau Field – Mike Roemer/AP

Cyber-physical Systems in Stadiums

- Recent report by CNBC (Nov. 2013) names five large sports stadiums running a particular industrial control system software with known vulnerabilities.
- Include Bryant-Denny Stadium (University of Alabama) and Marlins Park (home of the Miami Marlins baseball team)
- Vulnerabilities supposedly addressed.

Bryant-Denny Stadium
Credit: wikipedia.org

Smart Grid Vulnerabilities

- ***How to attack a SCADA system (or a controller of the future)?***
  - Network-based attacks designed to exploit system flaws, unpatched systems, etc.
  - Once attacker gains a foothold in the target network, further exploitation can take place – attacker can expand their control over command and control systems and affect operations.

Smart Grid Vulnerabilities

- ***How to attack a SCADA system?***
  - Attackers can also establish footholds in networks by exploiting corporate client machines.
  - They can use social engineering techniques (e.g., emails with embedded links designed to dupe victims to access the links and download malicious code).
  - In many large organizations – according to our data -- as many as 98% of incoming emails are filtered out because they are suspicious.

Smart Grid Vulnerabilities

- ***How to attack a SCADA system?***
  - Attackers can use wireless technologies that are pervasive and invisible.
  - E.g.: There is a high risk for introduction of unauthorized, rogue wireless access points.

Smart Grid Vulnerabilities

- ***How to attack a SCADA system?***
  - Homeland security personnel are seriously concerned about terrorist attacks that are multi-pronged.
  - These include attacks that include both a physical and a cyber component.
  - A March 2008 Cyber Storm exercise, mandated by Congress, assessed the viability and impact of such an attack.

Smart Grid Vulnerabilities

- ***How to attack a SCADA system?***
  - Millions of computers worldwide are infected by “malware” and can become “bots” controlled by cyber criminals.
  - A “bot” is a compromised machine, acting alone.
  - A “botnet” is a network of bots, controlled by a malicious hacker.
  - Attackers use botnets to:
    - ➢ Launch identity theft
    - ➢ Commit “click fraud” to fraudulently click on a purchase or ad
    - ➢ Most relevant – launch “denial of service attacks” that inundate computers with irrelevant materials.

Smart Grid Vulnerabilities

- Cyber crime is the "growth area" for law enforcement (FBI)
- Attacks on SCADA systems are a special concern.
- FBI has issued new regulations requiring mandatory reporting of any events of concern involving such systems.
- Goal: use the reports to do "follow-up" and "hardening"

Smart Grid Vulnerabilities

- Cyber attacks are an international concern
- Adversaries can launch sophisticated "information warfare"
- Can destroy critical infrastructure
- E.g., pro-Russian cyberattacks on Estonia
  – Estonia one of world's highest users of Internet technology
  – Attacks crippled vital daily functions.

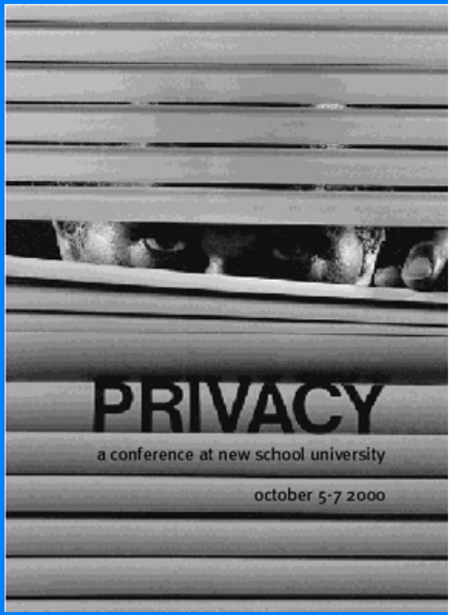
Smart Grid Vulnerabilities

- Cyber attacks are an international concern
- E.g., "botnet" attacks on South Korean government and private industry sites.
- In 2007, Scotland Yard uncovered an Al Qaeda plot to infiltrate and destroy a high-security Internet hub in the U.K., with apparent goal of a cyber attack designed to undermine the U.K.'s economic and business sectors.

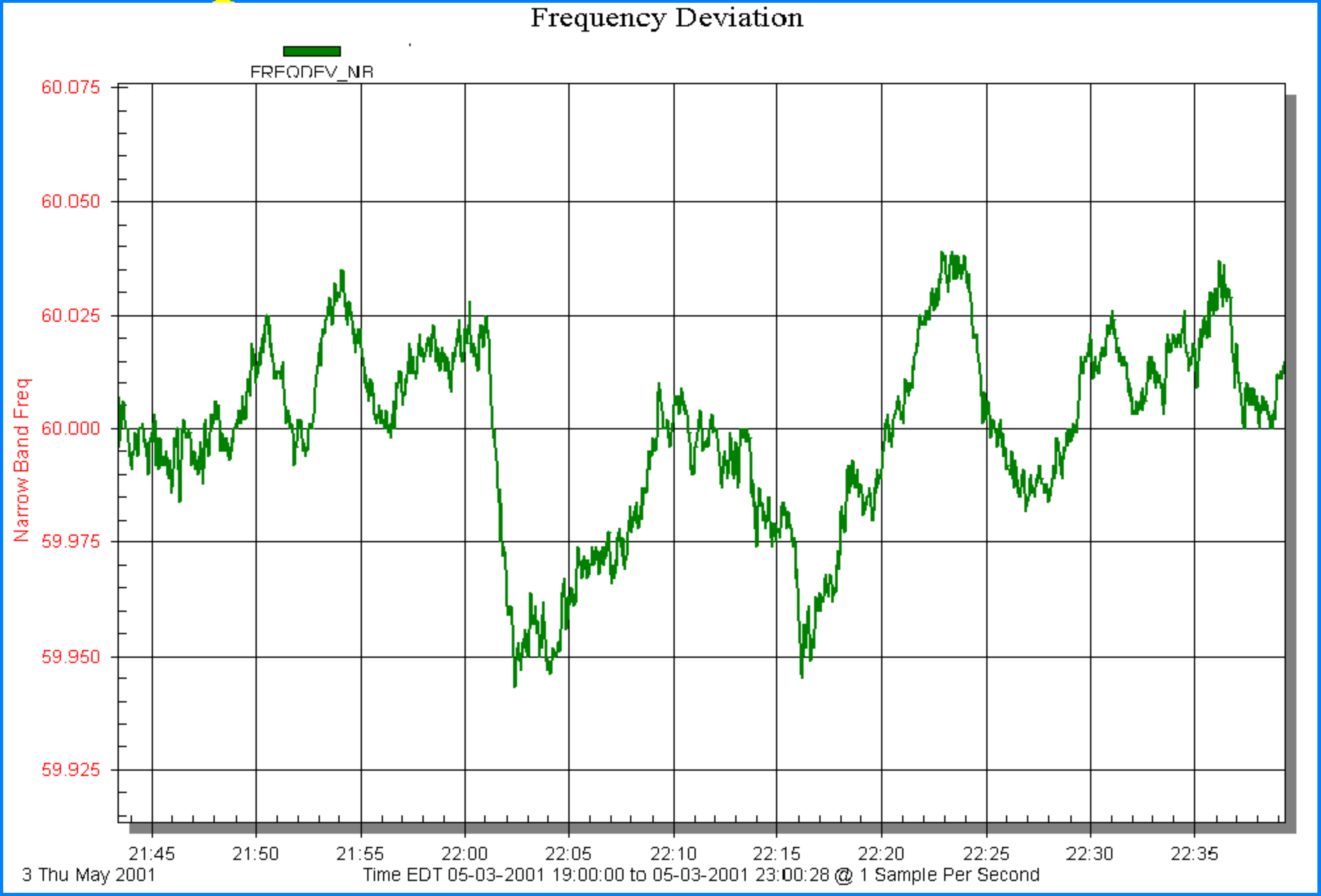
Smart Grid Vulnerabilities

•Phasor technology and phasor measurements provide additional data:

- –Such measurements will allow rapid understanding of how customers are using electricity.
- –But this raises privacy issues:
  - ➢Is customer on vacation?
  - ➢What movie is customer watching?



Last Episode of TV Series "Survivor"



An electronic "signature"

Source: Jim Ingleson (NYISO) and Joe Chow (RPI) via Massoud Amin

Smart Grid Vulnerabilities

- Privacy research is another area of emphasis at DIMACS and CCICADA

CCICADA
Command, Control, and Interoperability Center for Advanced Data Analysis
A Department of Homeland Security Center of Excellence

DIMACS
Center for Discrete Mathematics & Theoretical Computer Science
Founded as a National Science Foundation Science and Technology Center

ADT and Smart Grid: Research Challenges

Rapid System Understanding:

•Need to develop reliable, robust models to help us achieve system understanding given massive amount of relevant data that is collected.

•Need a new mathematics for characterizing uncertainty in information created from the large volumes of data arising from the smart grid.

ADT and Smart Grid: Research Challenges

Rapid System Understanding:

- Need new methods to enable the use of high-bandwidth networks by dynamically identifying only the data relevant to the current information need and discarding the rest.

ADT and Smart Grid: Research Challenges

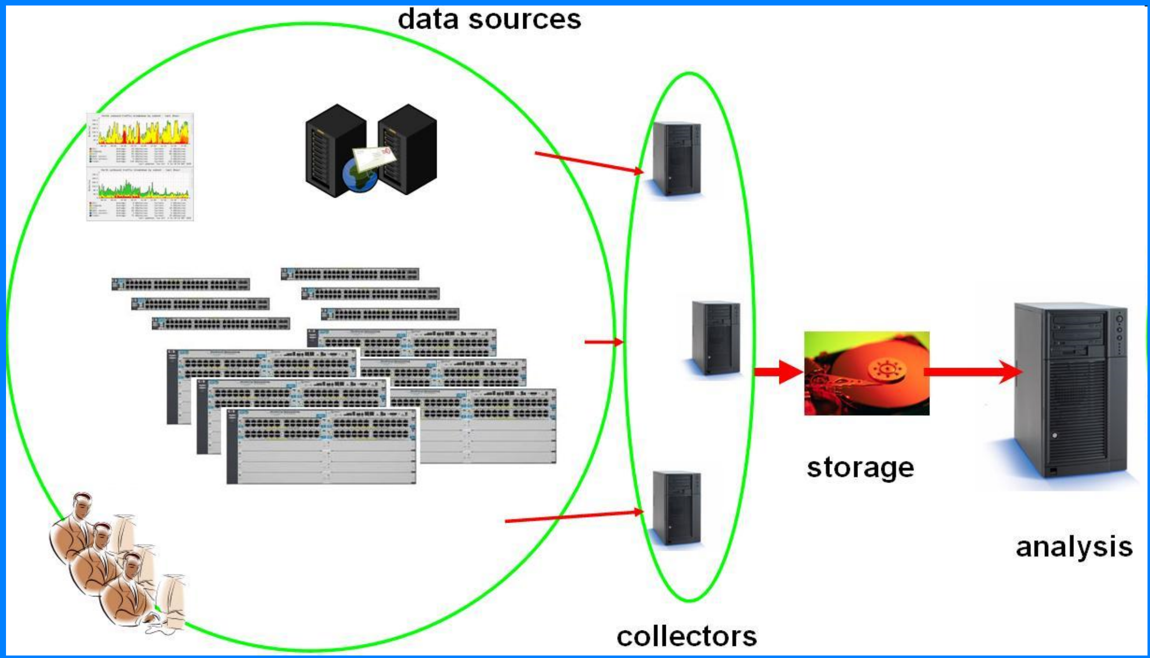
Transmission Reliability:

- Wide area situational awareness and advanced computational tools can help with quick response to dynamic process changes, e.g., using automatic switching.
- Sample challenge: How far are we from the edge? When voltages drop too fast, the entire power system can collapse.

ADT and Smart Grid: Research Challenges

Anomaly Detection:

•New algorithmic methods are needed to understand, process, visualize data and find anomalies rapidly.



ADT and Smart Grid: Research Challenges

Grid Robustness:

- How can we design "control" procedures so that the grid can quickly and efficiently respond to disturbances and quickly be restored to its healthy state?
- Need fast, reliable algorithm to respond to detected problem.
  - Should not necessarily require human input
  - Has to be able to handle multiple possible "solutions"
  - Has to be able to understand what to do if all possible solutions are "bad"

ADT and Smart Grid: Research Challenges

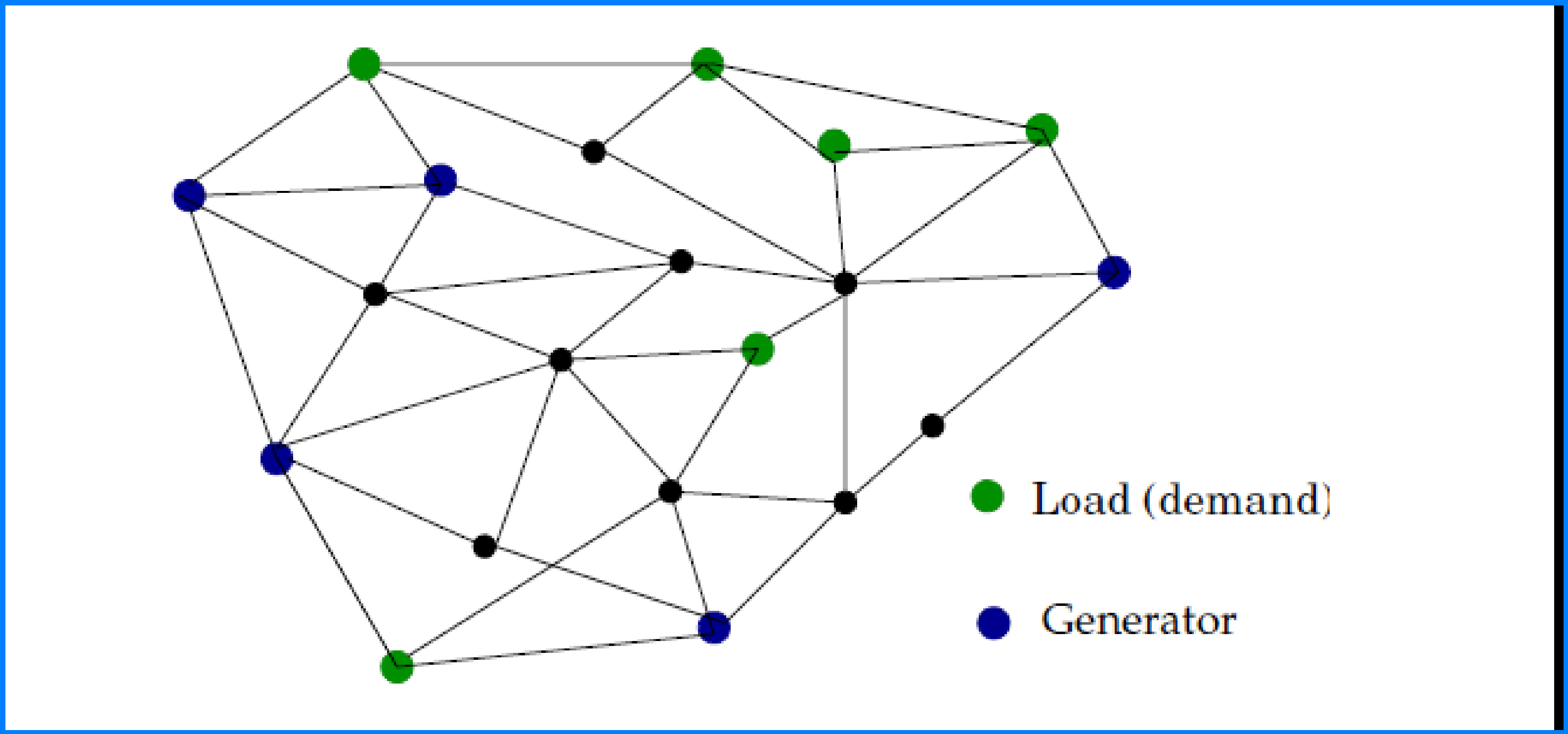
Grid Robustness:

- Tool of interest: cascade model of Dobson, et al.
  - An initial “event” takes place
  - Reconfigure demands and generator output levels
  - New power flows are instantiated
  - The next set of faults takes place according to some stochastic model

ADT and Smart Grid: Research Challenges

Grid Robustness:

Cascade Model (Dobson, et al.)

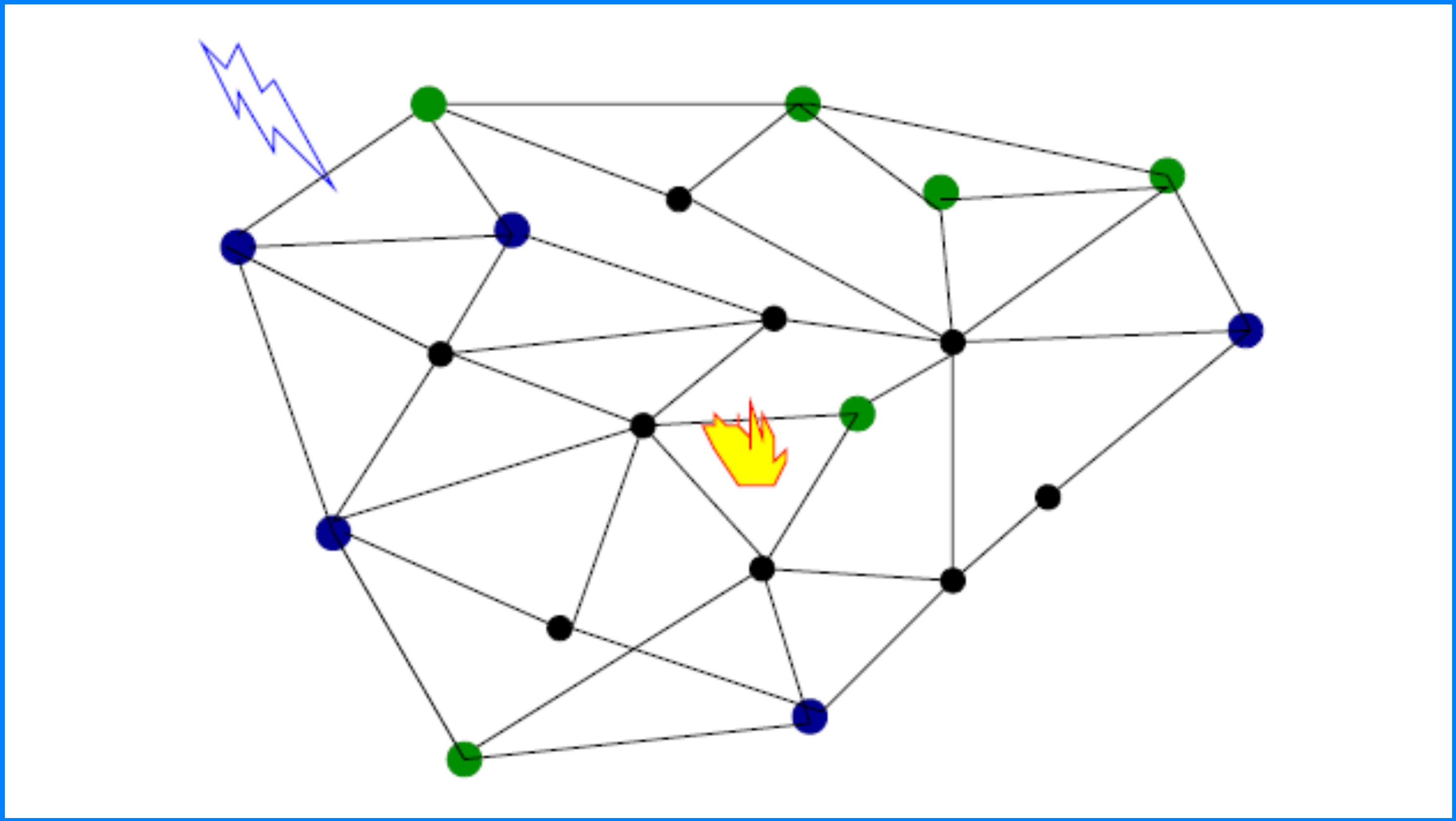


Credit: Daniel Bienstock

ADT and Smart Grid: Research Challenges

Grid Robustness:

Cascade Model (Dobson, et al.)

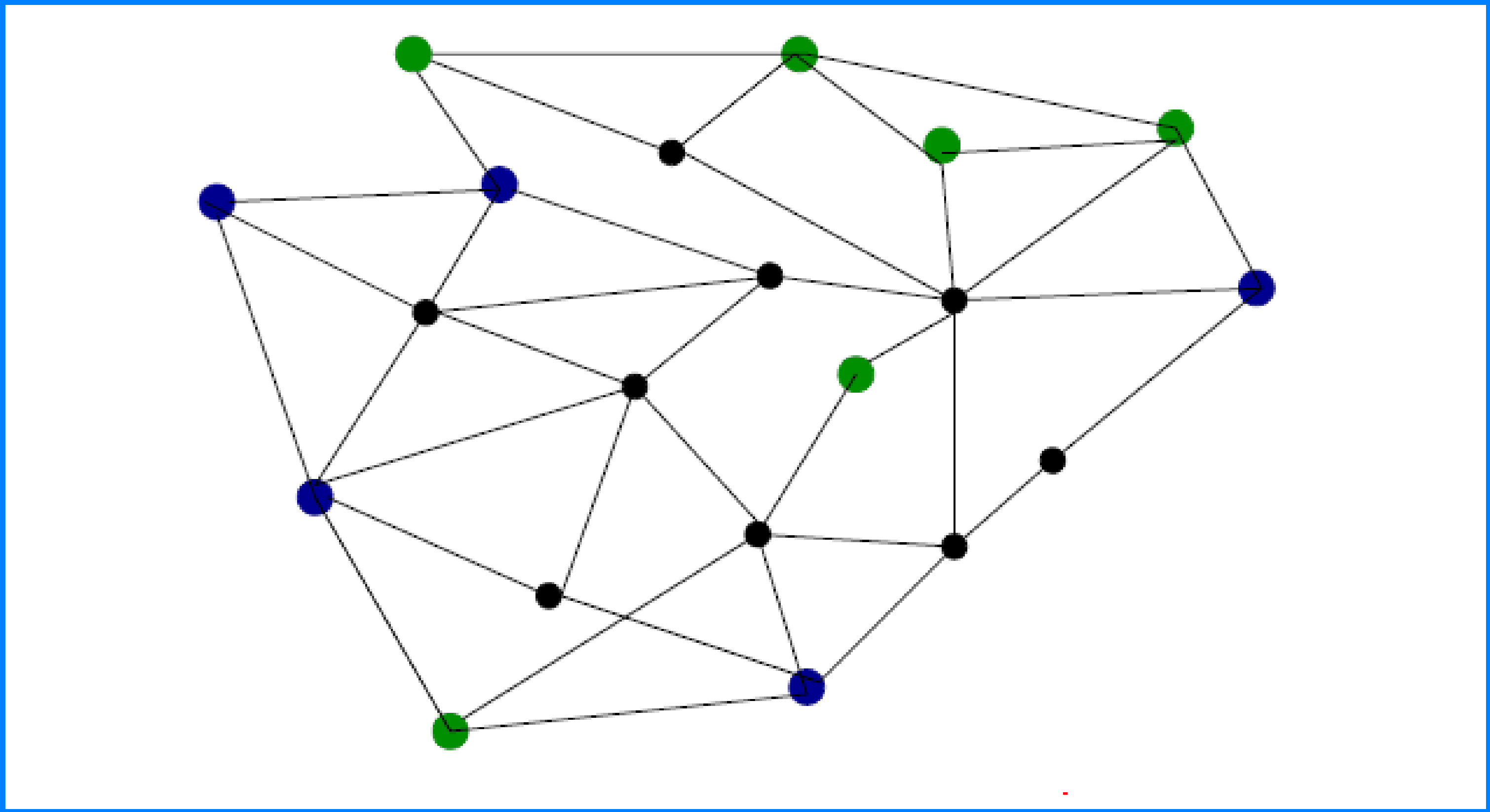


Credit: Daniel Bienstock

ADT and Smart Grid: Research Challenges

Grid Robustness:

Cascade Model (Dobson, et al.)

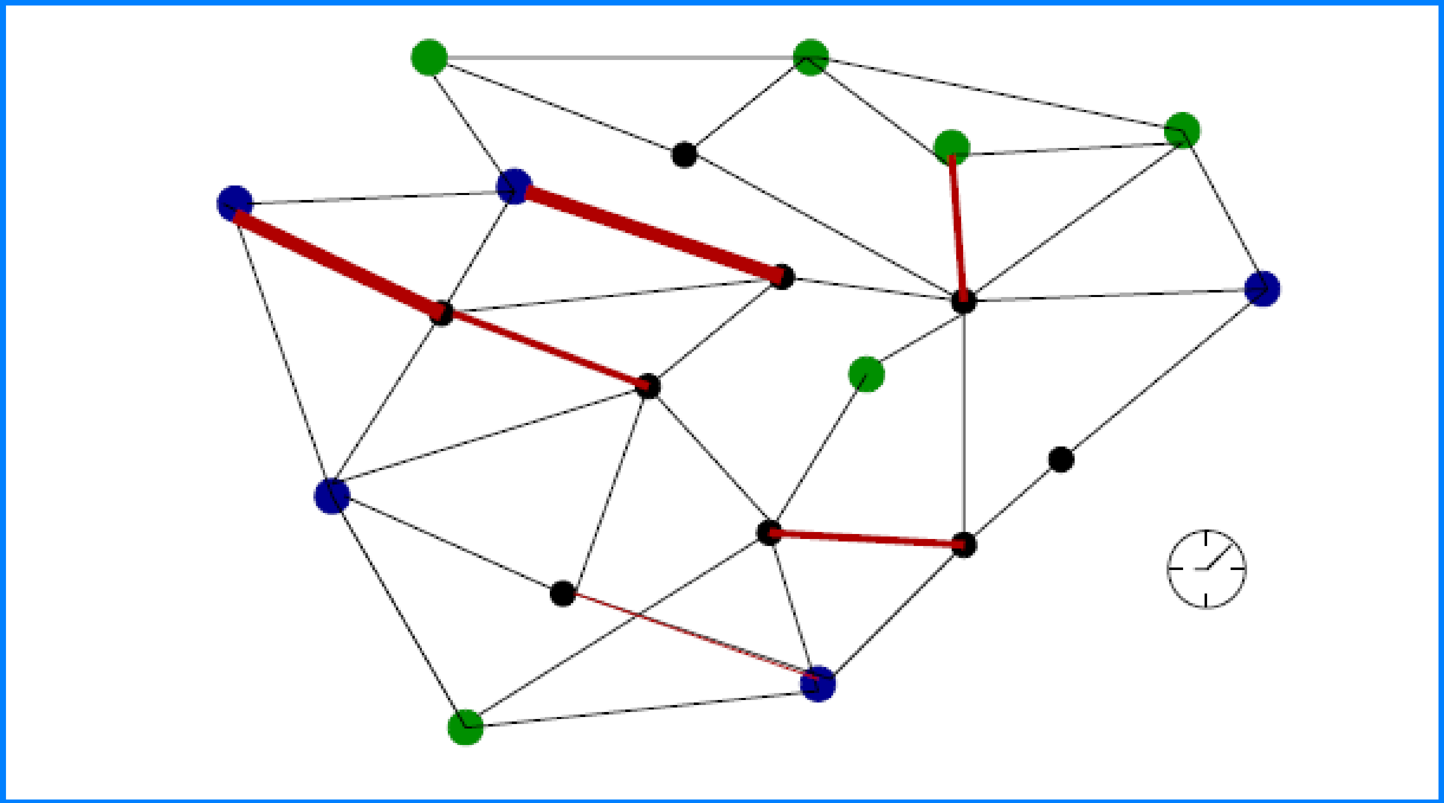


Credit: Daniel Bienstock

ADT and Smart Grid: Research Challenges

Grid Robustness:

Cascade Model (Dobson, et al.)



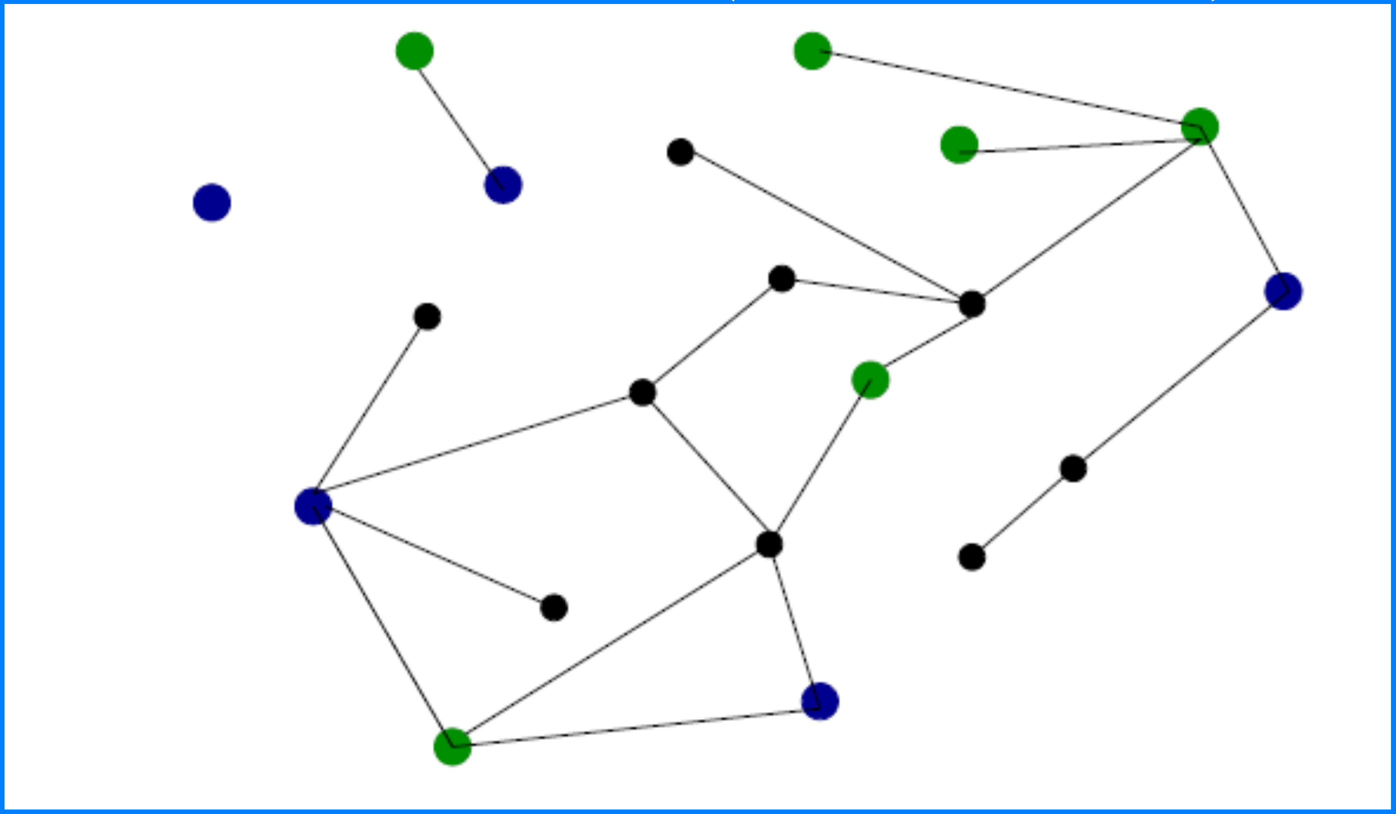
Credit: Daniel Bienstock

Increased flows on some lines

ADT and Smart Grid: Research Challenges

Grid Robustness:

Cascade Model (Dobson, et al.)

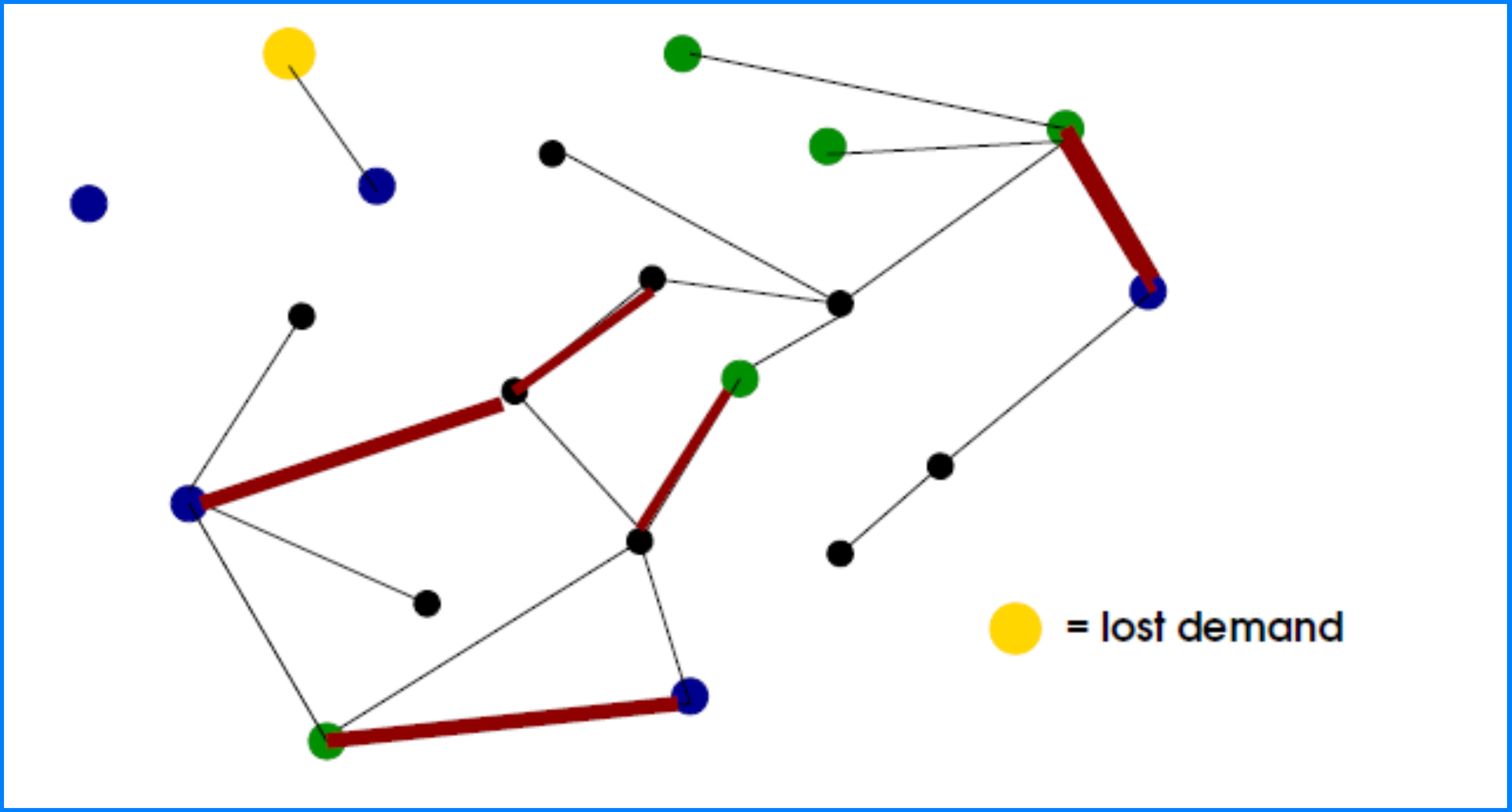


Credit: Daniel Bienstock

ADT and Smart Grid: Research Challenges

Grid Robustness:

Cascade Model (Dobson, et al.)

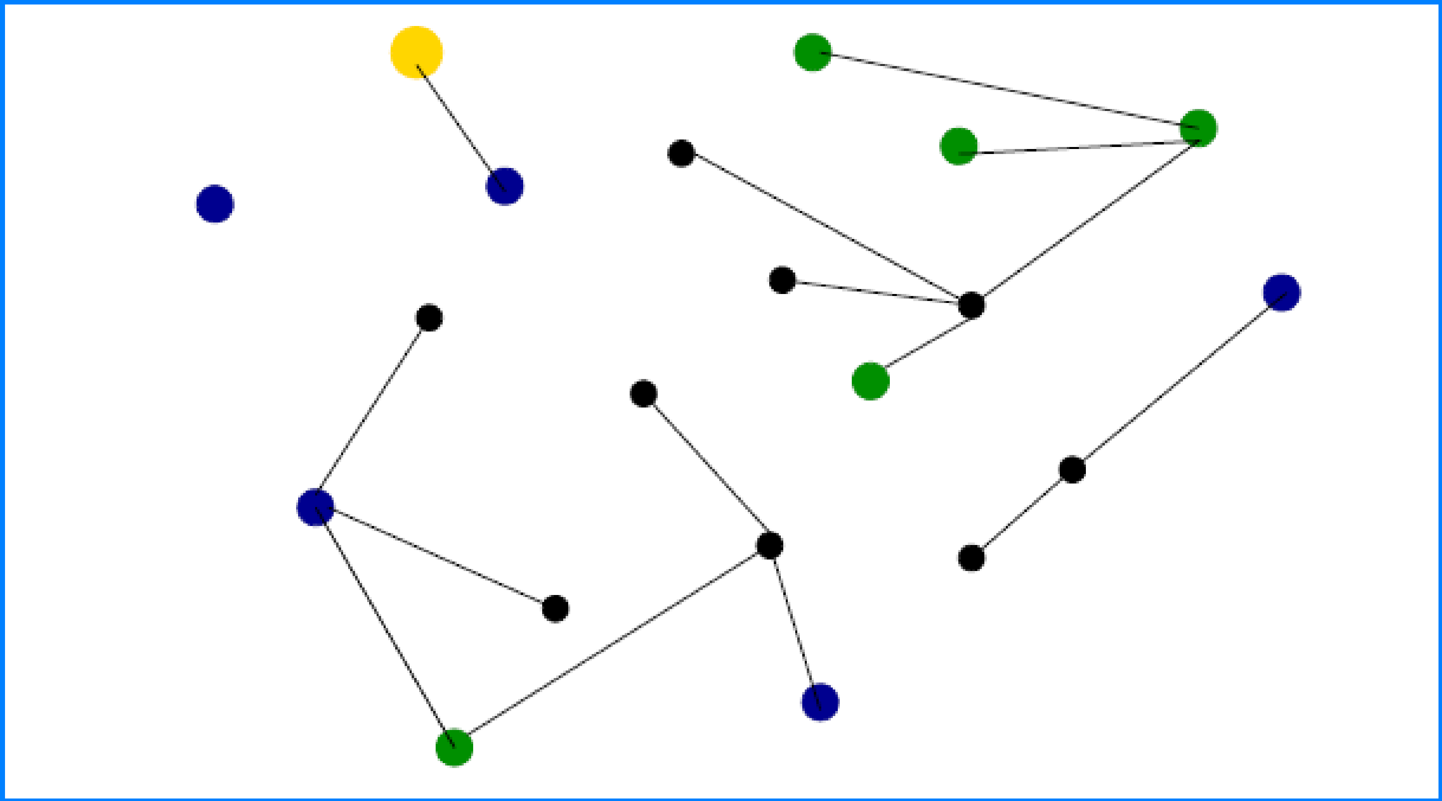


Credit: Daniel Bienstock

ADT and Smart Grid: Research Challenges

Grid Robustness:

Cascade Model (Dobson, et al.)

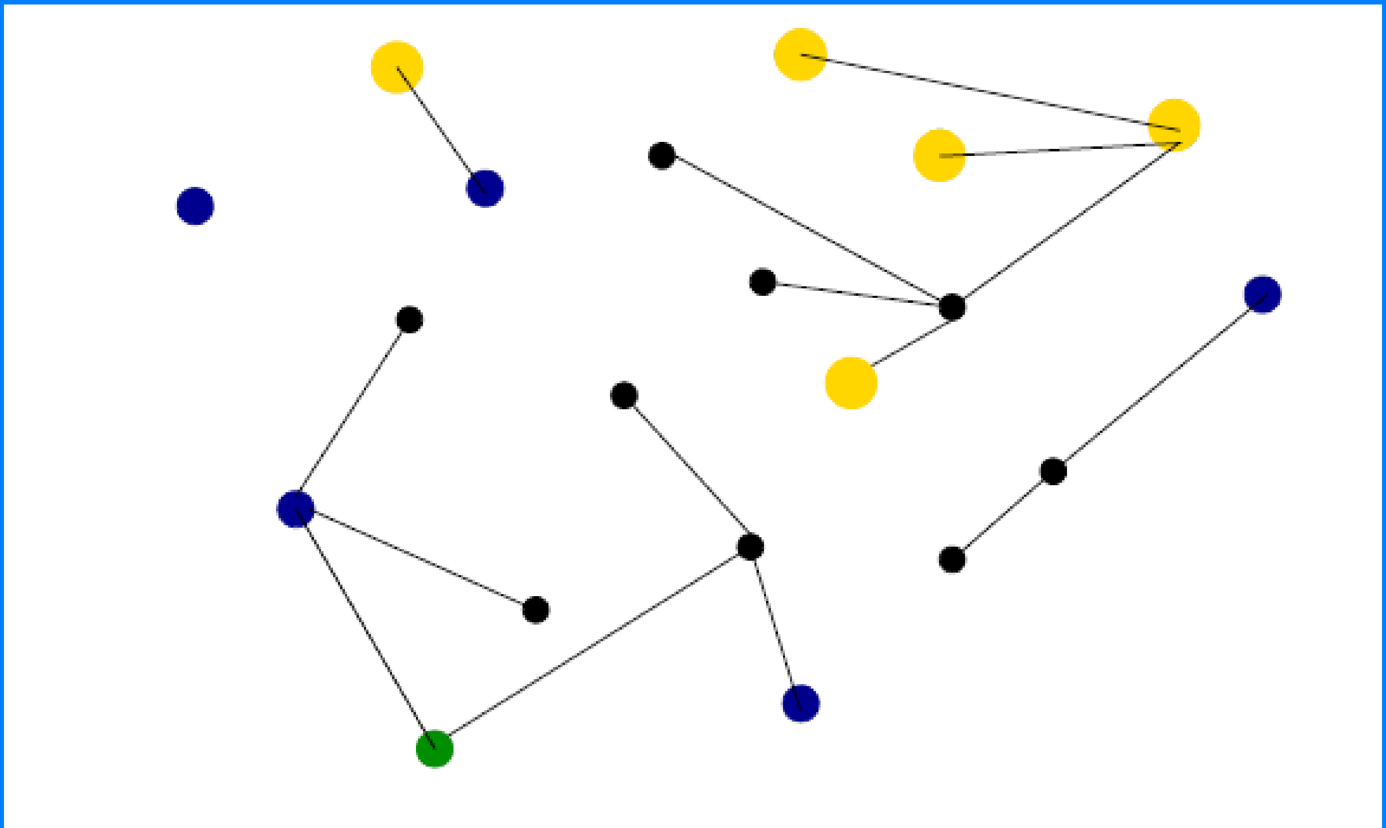


Credit: Daniel Bienstock

ADT and Smart Grid: Research Challenges

Grid Robustness:

Cascade Model (Dobson, et al.)



Credit: Daniel Bienstock

ADT and Smart Grid: Research Challenges

Grid Robustness:

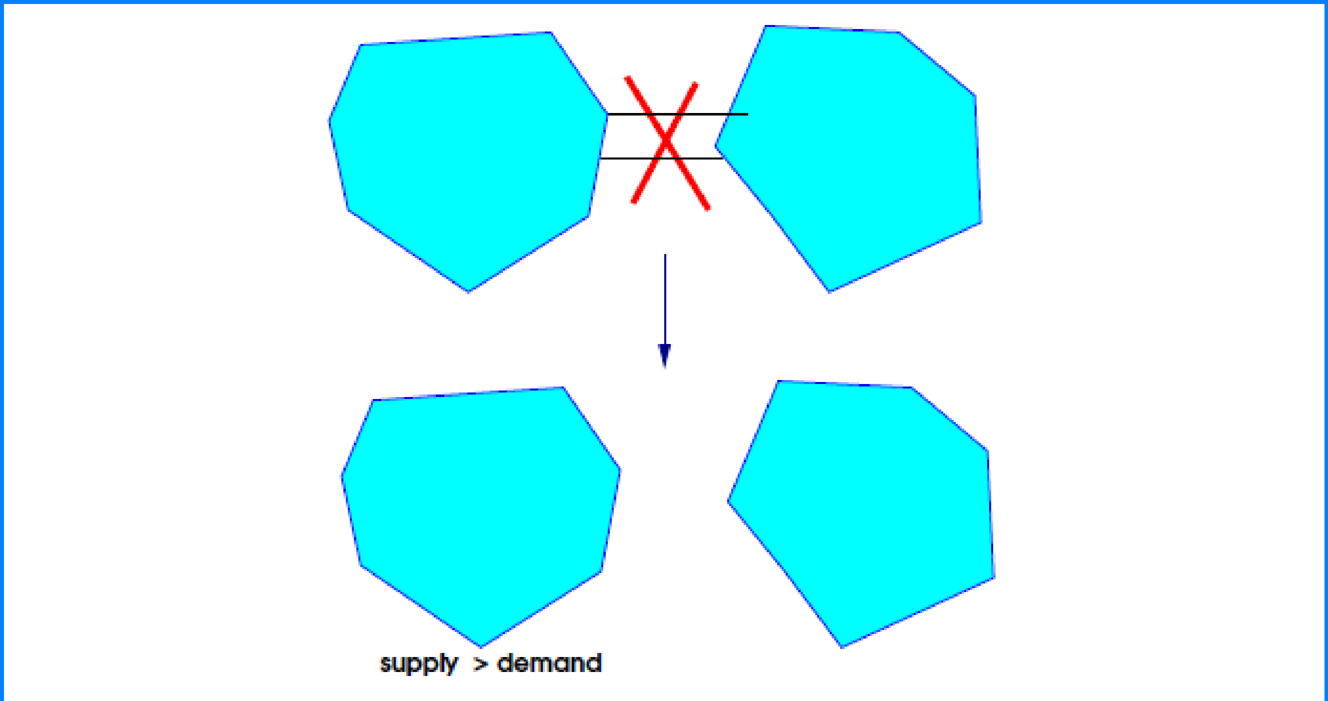
- Cascade model of Dobson, et al.: Exercising "Control"
  - –An initial "event" takes place
  - –Reconfigure demands and generator output levels
  - –New power flows are instantiated
  - –Instead of waiting for the next set of faults to take place according to some stochastic process, use the cascade model to learn how to:
    - ➢Take measurements and apply control to shed demand.
    - ➢Reconfigure generator outputs; get new power flows

ADT and Smart Grid: Research Challenges

Grid Robustness:

Cascade Model (Dobson, et al.)

•Use Model to Learn how Best to Create Islands to Protect Part of the Grid



Credit: Daniel Bienstock

ADT and Smart Grid: Research Challenges

Grid Robustness:

- How does the fact that the current power grid has grown up haphazardly and is dynamically changing enter into our "control" protocols?
- The current grid operates "close to the edge." How does that affect control protocols?

ADT and Smart Grid: Research Challenges

Developing Self-healing Systems:

- Need efficient monitoring and probing (without overwhelming system resources)
- Require statistical prediction of impending problems
- Develop automatic derivation of inter-component dependency information
- Need problem location and probe selection
- Develop automated planning and learning of corrective action workflows

ADT and Smart Grid: Research Challenges

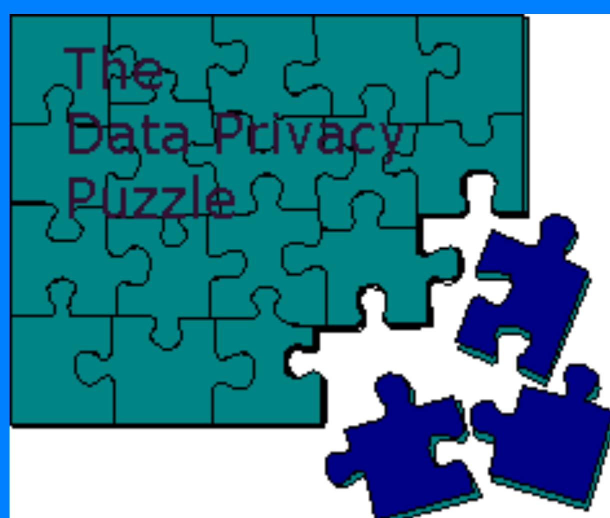
Cybersecurity:

- Resilient and secure grid systems require:
  - Secure and real-time communication protocols
  - Automated attack response systems
  - Regular risk and security assessment
- Sample challenge: design "message authentication" protocol for SCADA.

ADT and Smart Grid: Research Challenges

Privacy:

- We need to develop tools for protecting the privacy of individuals under new data collection methods
- Otherwise, there will be serious opposition to implementing smart meters and other changes



ADT and the Smart Grid

- Development of the smart grid has great promise for helping us make our electric power system more efficient and less vulnerable.
- It can also help users of electric power operate more efficiently and frugally.
- ADT can help in the design of the smart grid.
- ADT is also critically important in addressing the vulnerabilities that could make development of the smart grid a liability