Future Grid Initiative White Papers on the Information Hierarchy for the Future Grid: Conclusions and Research Directions

Presented by

Peter W. Sauer

University of Illinois at Urbana-Champaign

PSERC Webinar
November 6, 2012

Networked Information Gathering and Fusion for Wide-Area Monitoring and Control: A Middleware Communication View

Junshan Zhang and Vijay Vittal
Arizona State University

Peter W. Sauer
University of Illinois at Urbana-Champaign

PSERC

Motivation

- Smart grid requires a wide-area monitoring and control system to ensure:
  - Secure and reliable operation
  - Protection from contingencies

- State-of-the-art for Supervisory Control and Data Acquisition (SCADA) system:
  - Operate in a centralized fashion, using a hierarchical control system
    - ✓ i.e., the control center gathers data from sensors and sends commands to control devices
  - Communication infrastructure for power grid has star topology:
    - ✓ Each substation communicates directly to the control center
  - Not scalable and hence is used for local monitoring and control
  - Not robust, in the sense that when one node fails, the subtree associated with it would be disconnected from the network

Motivation (Cont'd)

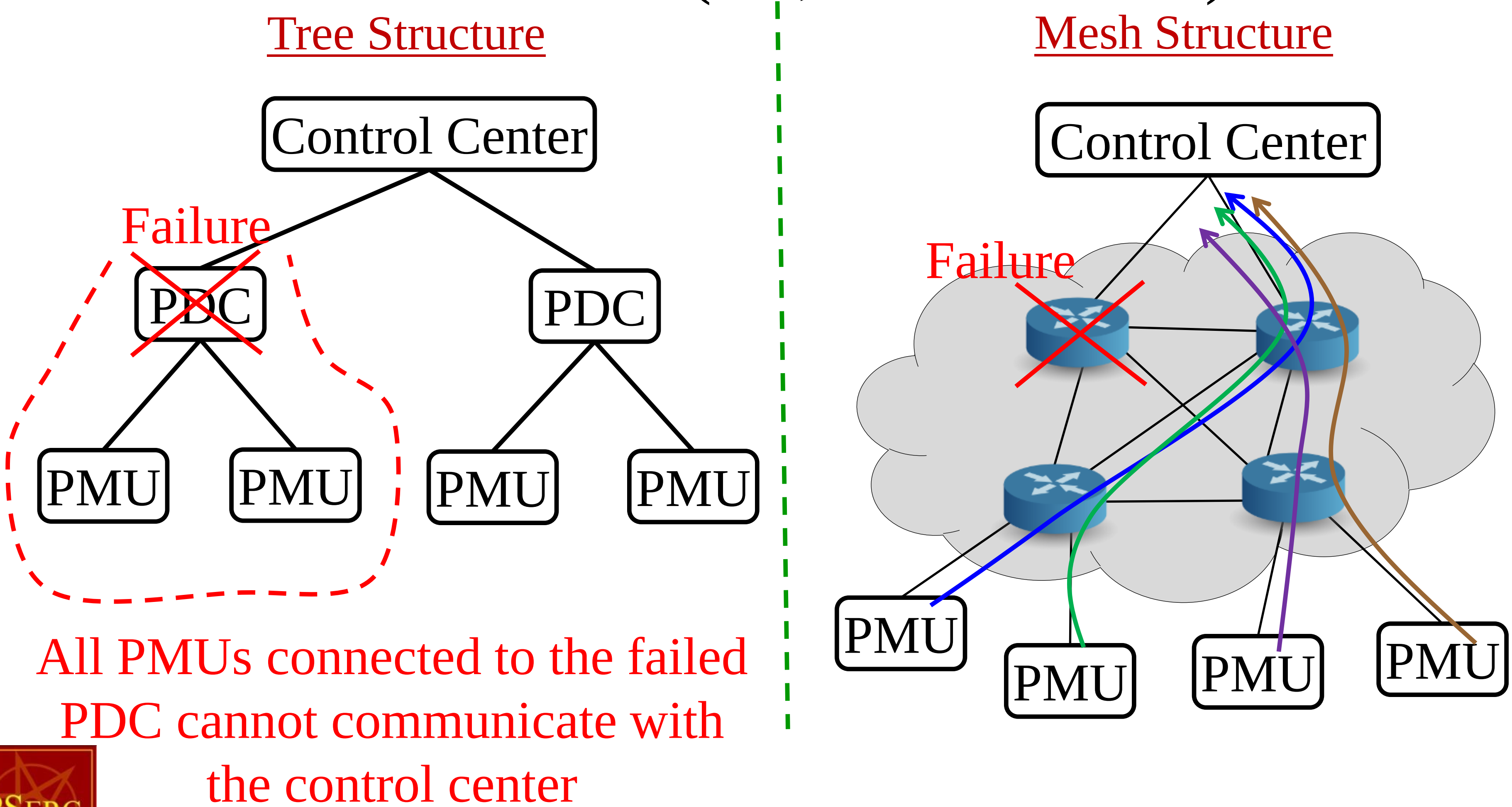
- Hierarchical tree structure for wide-area monitoring and control
  - ❖ For example, phasor network established by Bonneville Power Administration (BPA) in 2000, with three levels of hierarchy:
    - ✓ 1st level: Phasor Measurement Units (PMUs)
    - ✓ 2nd level: Phasor Data Concentrators (PDCs) for local-level data collection
    - ✓ 3rd level: SCADA system for the control center
  - ❖ Limitations:
    - ✓ Not suitable for time-critical data delivery
      - ❑ Due to the bottlenecks incurred at high-level nodes (i.e., PDCs/Super-PDCs)
    - ✓ Vulnerable to node/link failures and attacks by adversaries
      - ❑ Since the system relies on a (relatively) small number of high-level nodes and their associated links for the entire system to function

➡ Smart grid requires a cost-effective, reliable and resilient communication system for wide-area monitoring and control

PSERC

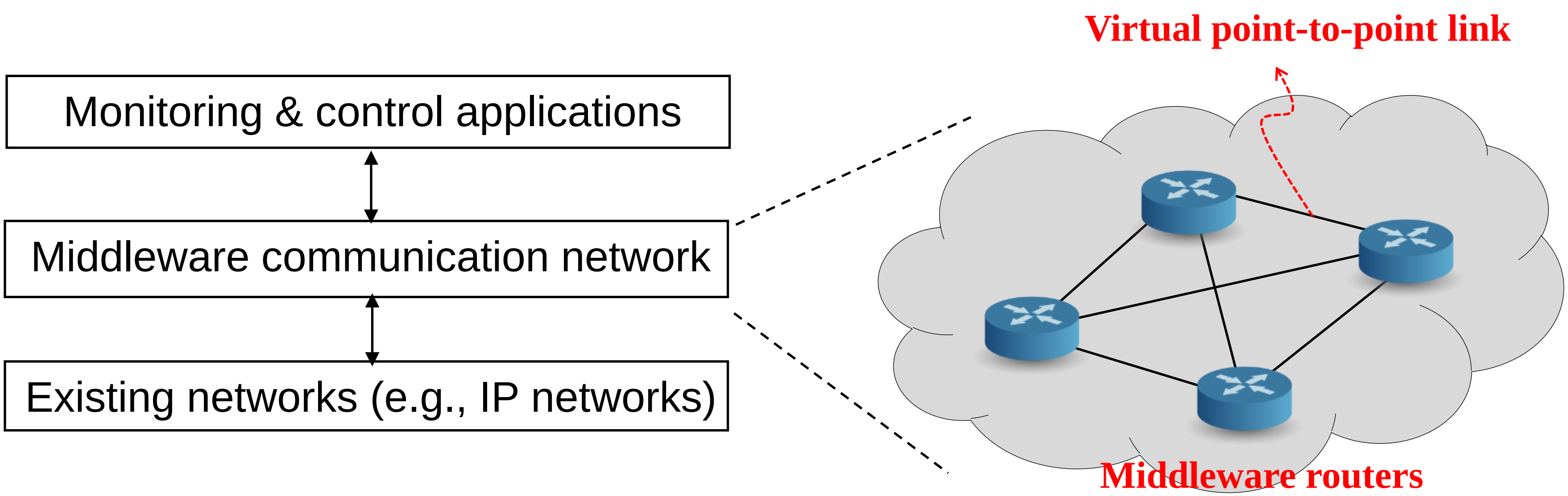
Motivation (Cont'd)

- Mesh information structure: More robust than hierarchical structure (i.e., tree structure)



Middleware Communication System

- Overlay network consisting of *middleware routers*
  - ✓ Built upon the existing (heterogeneous) communication networks
  - ✓ A "virtual" link between two middleware routers can be an actual point-to-point link or even a network (e.g., IP or cellular network)
- Efficiently manages underlying communication resources to deliver data and meet QoS requirements of smart grid



Research Objectives

- Goal: develop an efficient, reliable and resilient middleware communication framework for smart grid
- In designing such a framework, we will address design issues, including:
  - ✓ Cost-effective deployment of a reliable and resilient middleware communication system
  - ✓ Efficient allocation and management of the underlying network resources for a QoS-guarantee middleware communication system
  - ✓ Network management of middleware routers (for packet scheduling and routing) to achieve high throughput and low latency, with given network resources
  - ✓ Efficient flow control for adapting data-injection rates for multiple information flows
    - When network congestion occurs

Cyber Physical Systems Security for Smart Grid

Manimaran Govindarasu
Iowa State University
(gmani@iastate.edu)

Pete Sauer
University of Illinois at Urbana-Champaign
(psauer@illinois.edu)

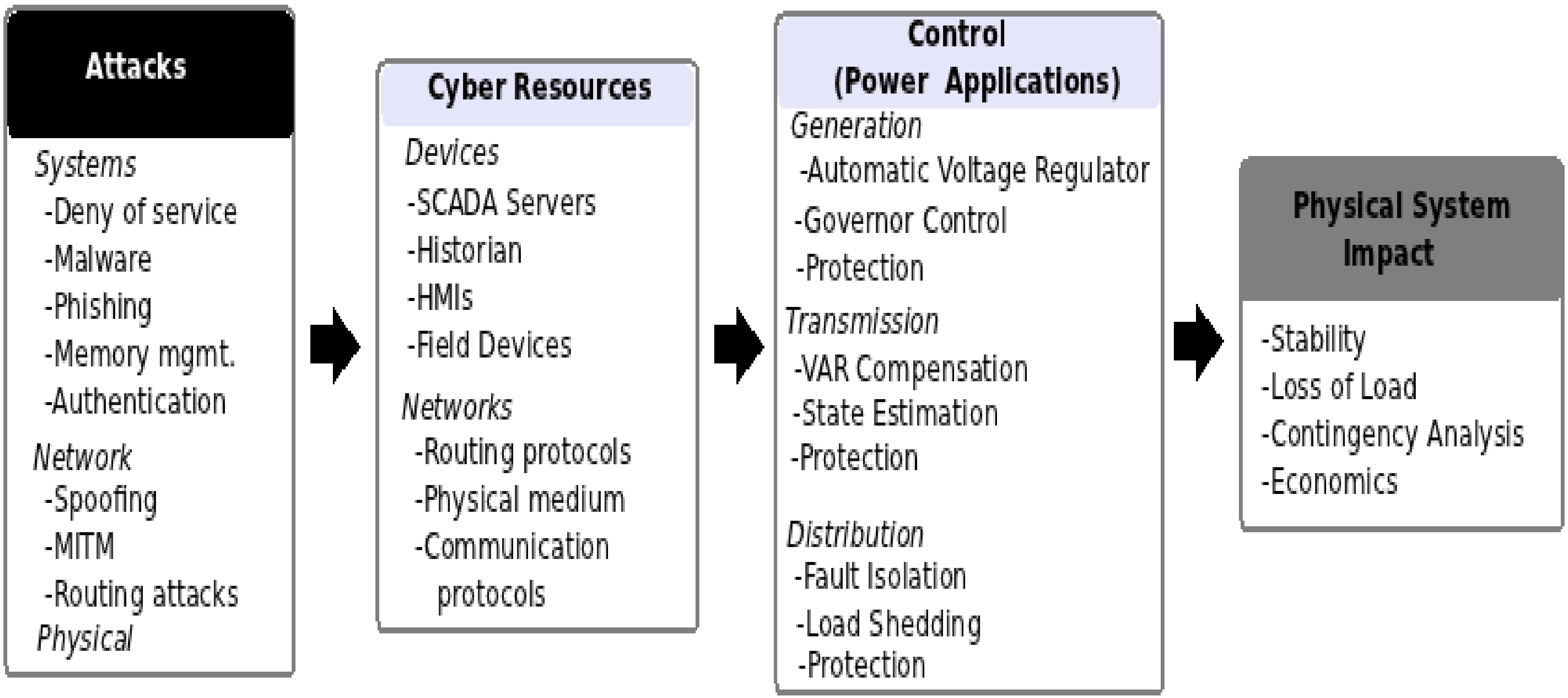
PSERC

Key research topics

1. Defense against HILF cyber events
2. Attack-resilient WAMPAC
3. Quantitative risk assessment
4. Cyber-physical testbeds & validation

PSERC

Attacks-Cyber-Control-Physical Relationships



Defense against HILF cyber events

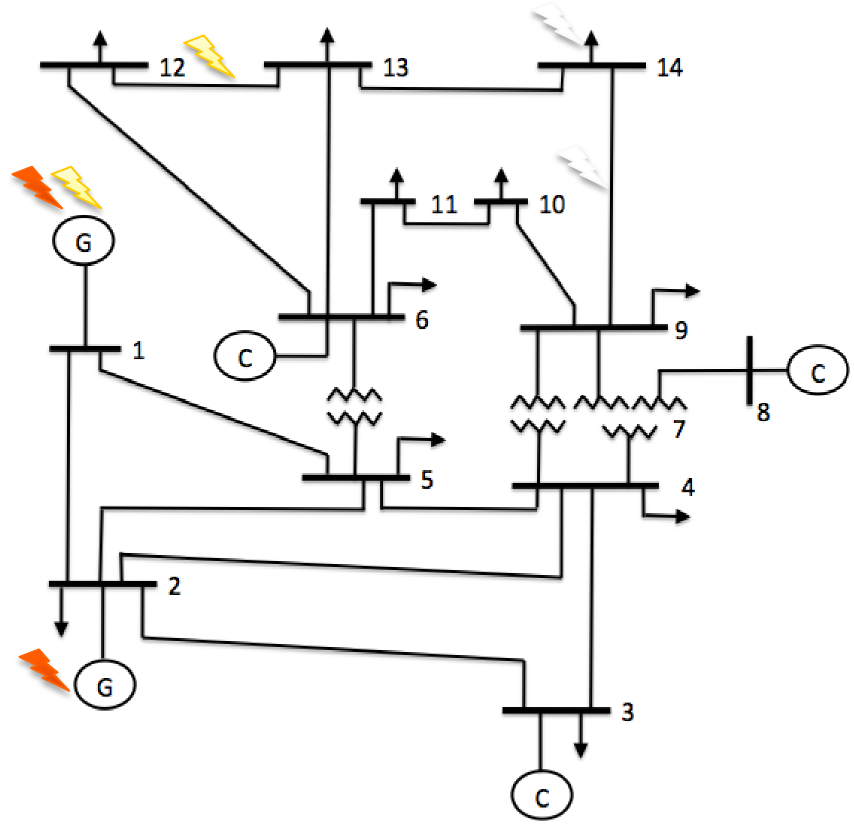
Smart coordinated attacks in space and time

Impacts: real-time operation, load loss, stability, market

Risk modeling & mitigation of coordinated attacks

Game-theoretic approach for attack-defense modeling

Plan beyond N-1 criteria



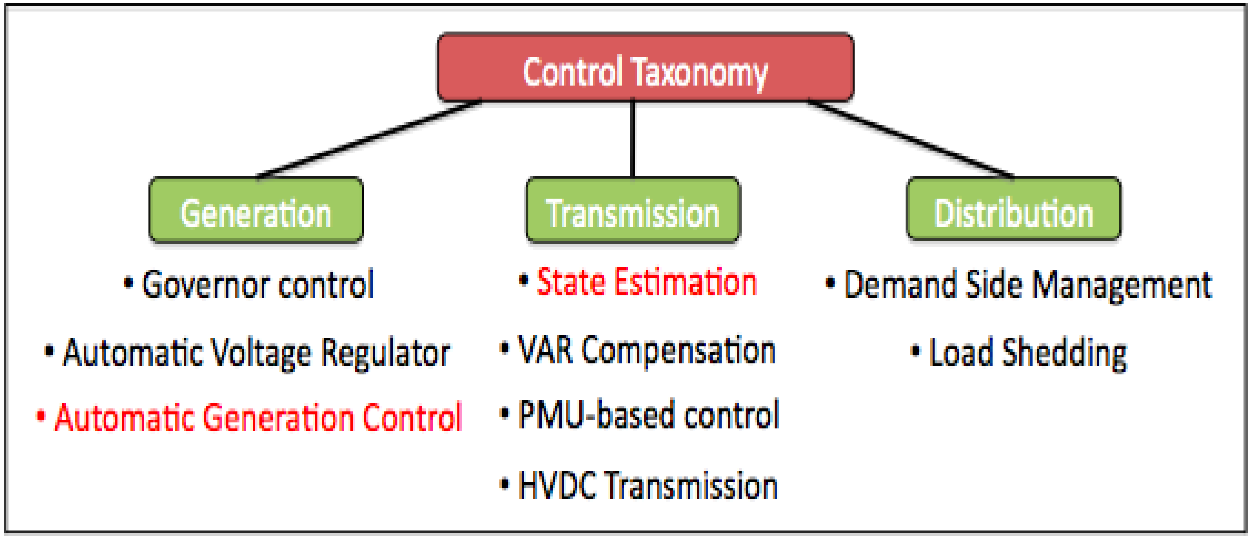
Game theoretic approach to Cyber-Physical system security

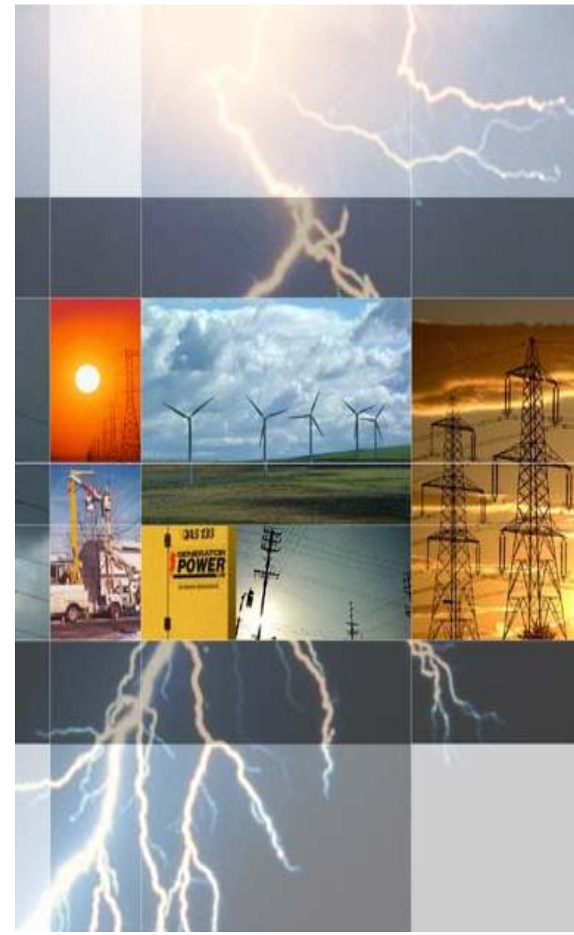
- **Mathematical framework**
  - Model coordinated attacks and attack resilient operations
  - Identify best operator responses for attack scenarios
- **Attacker/Defender characterization based on game formulation**
  - Cooperative/Non-cooperative game
  - Bayesian game with uncertainties
  - Dynamic, learning based formulations
- **Attack impact captured as a cost & best defense strategies**
  - Load loss
    voltage stability
    line flow violations
    cascading failures
  - Defense & Security investments for attack scenarios

PSERC

Attack-resilient WAMPAC

"Transform fault-resilient grid to attack-resilient grid"





Quantify attack impacts on power system control loops
Robust Cyber-Physical Defense algorithms

Domain specific Anomaly Detection

Model based control approach

Attack resilient control: AGC

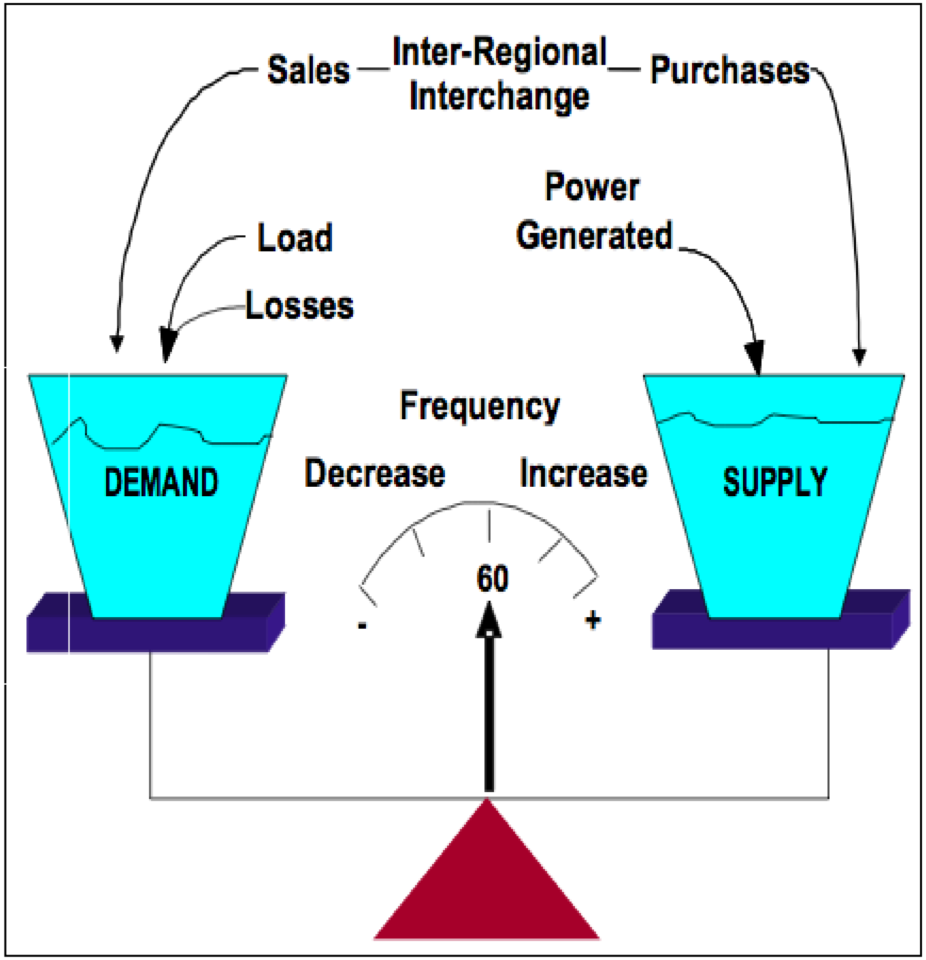
Attack vector: Modify tie-line flow and frequency measurements

Impact: Abnormal operating frequency conditions

Anomaly Detection:

- Load Forecasts
- Topology information
- Attack Templates
- System Data
- System Resources

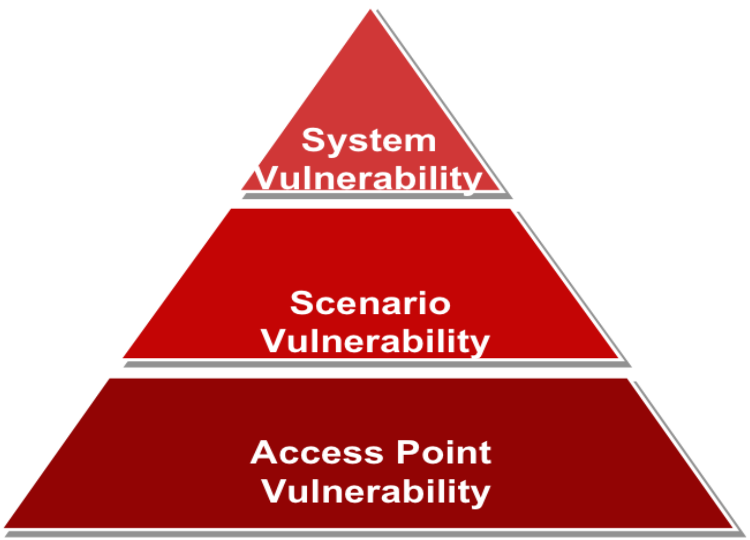
Model based control: Area Control Error based on load forecasts instead of actual load



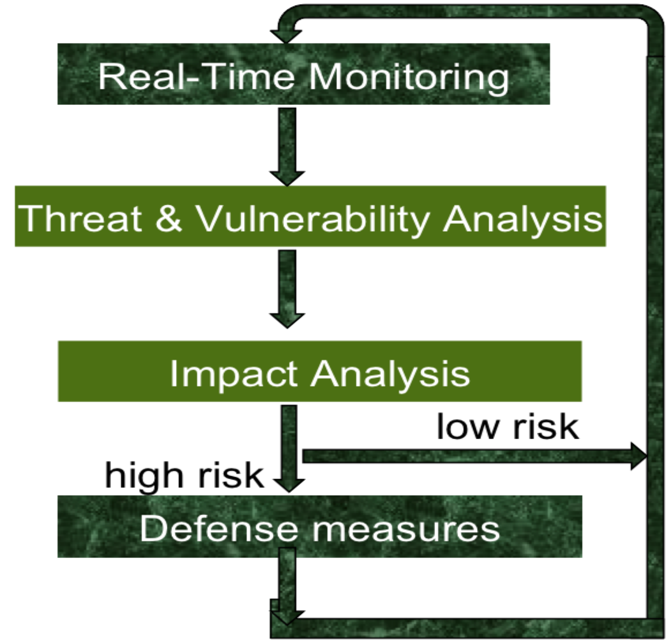
Risk modeling & Mitigation

Risk = Threat x Vulnerability x Impacts

- **Risk Assessment & Risk Mitigation (GAO CIP Report, 2010)**
- **Security Investment Analysis**



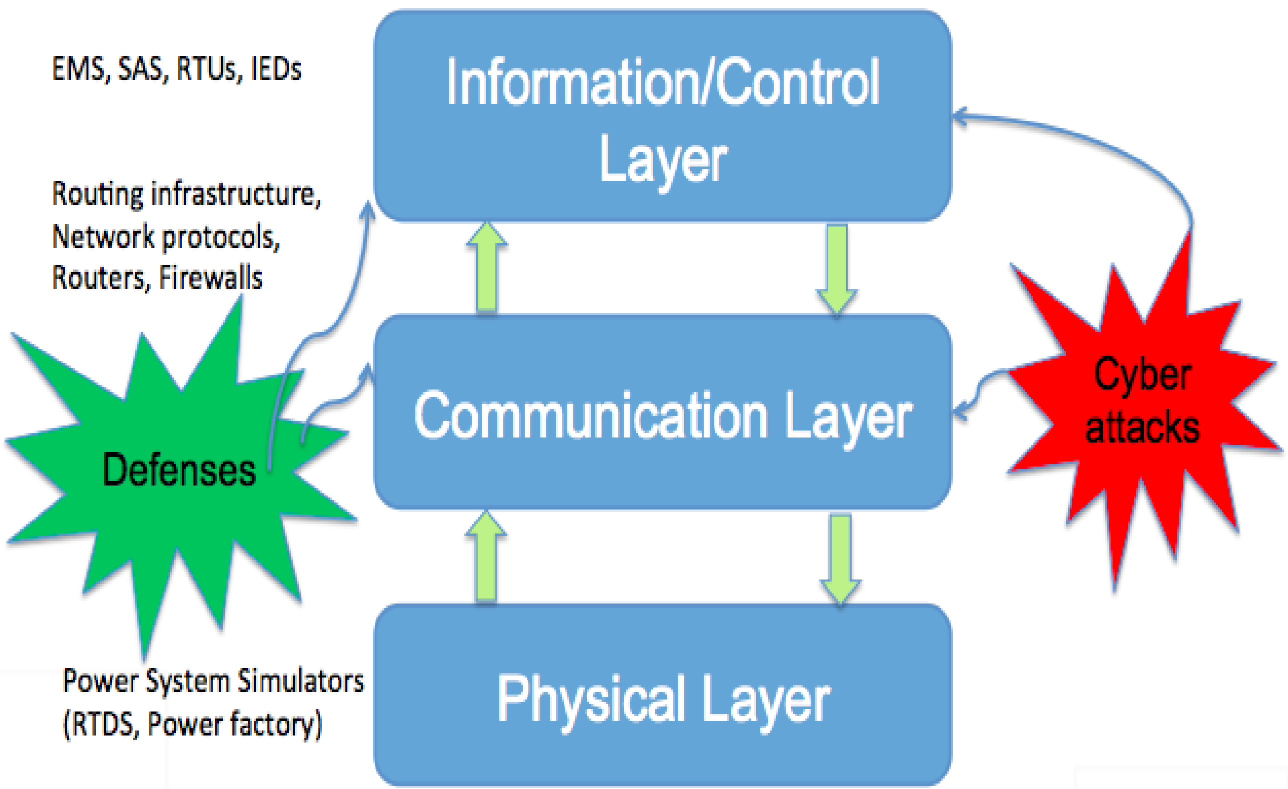
Hierarchical modeling



Need: Realistically accounting all three – threat, vulnerability, impacts

Cyber-Physical Testbed & Applications

"Need: National Smart Grid Cyber Security Testbed"



Risk Modeling & Mitigation

- Vulnerability assessment
- Impact analysis
- Risk assessment
- Defense algorithms

CPS Security Evaluations

- Smart attack vector formulation
- Attack-resilient WAMPAC

Vendor product testing

- Protocols, Firewalls, VPN
- Relays, Control Software

Federated Testbed – leverage existing testbeds at universities (ISU, UIUC, WSU) and DOE labs (INL, PNNL, ORNL)

Broad Analysis White Paper

AMI: Communication Needs and Integration Options

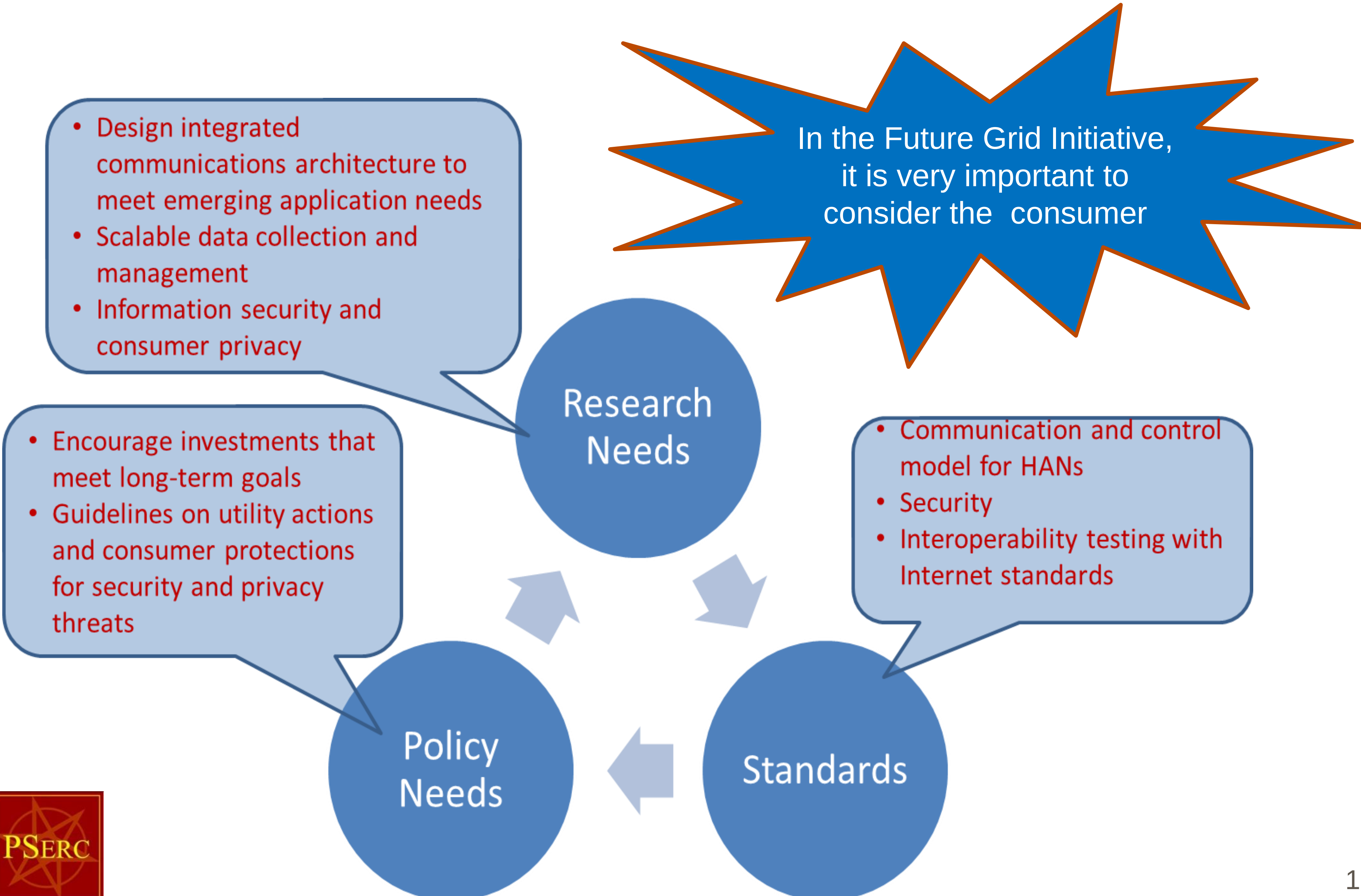
Future Research Need

A Secure and Privacy-aware Information-sharing Framework for Electricity Delivery

Vinod Namboodiri, Wichita State University

PSERC

Broad Analysis White Paper Summary



PSERC

Pressing Research Need

The design of a framework that leverages Information and Communication Technologies (ICT) to enable consumer participation for more efficient and cleaner electricity delivery considering two main aspects:

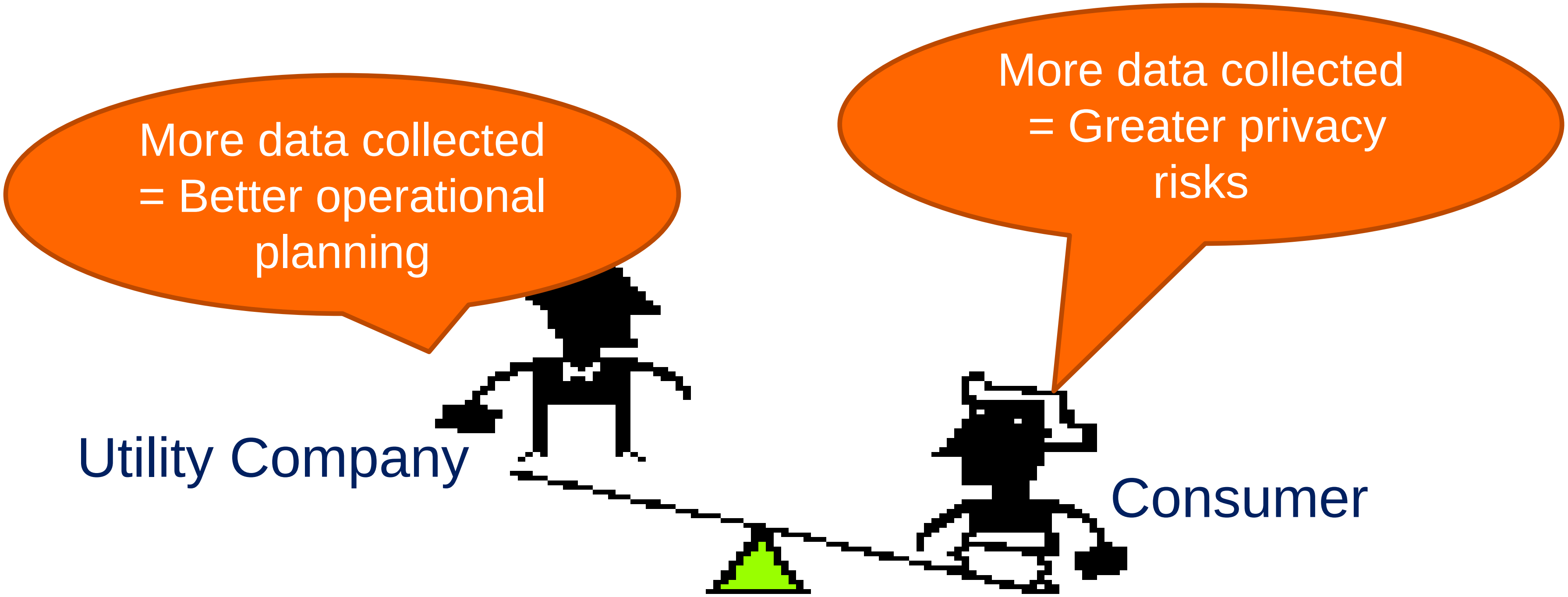
- Data volume
- Consumer privacy

Motivation

Current practice is a "piecemeal" approach

- One solution for one application scenario
- Not integrated across applications
- Information sharing needs and privacy are considered as independent problems

PSERC



A privacy-aware information sharing framework is needed that balances utility data needs with consumer privacy preservation.

A consumer-side big-data problem!

Handling Data Volume

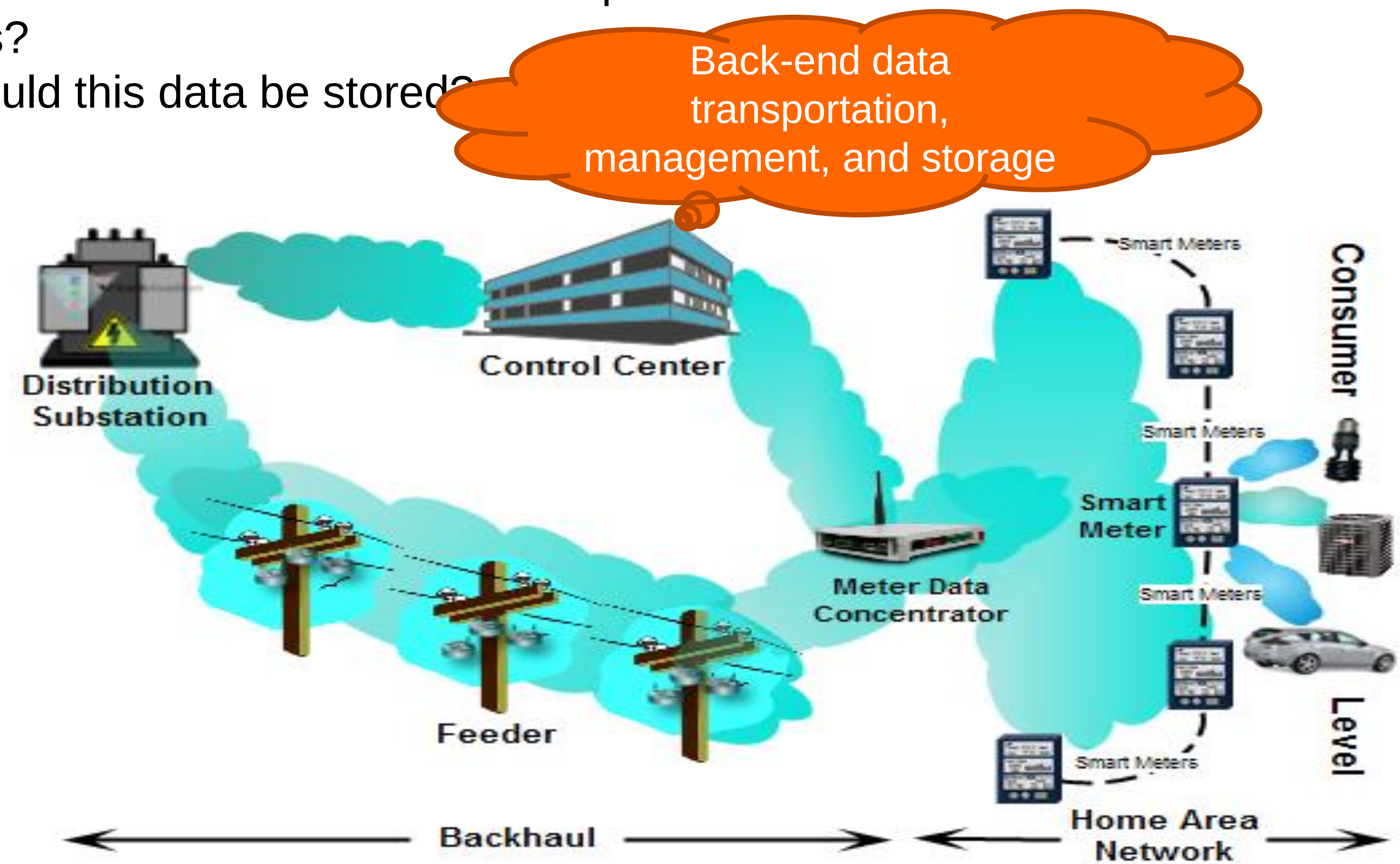
<u>Key Questions</u>

1. What data should be collected from consumers to aid operational planning?
2. What is the best communications architecture to collect this data from consumers?
3. Where should this data be stored?

Preserving Consumer Privacy

<u>Key Questions</u>

1. How can we quantify customer privacy in smart grids?
2. How can we make optimal information-sharing decisions based on this quantification?



(Blue cloud-like links indicate infrastructure needed)

Potential Benefits:

- Better utilization of planning tools developed to make optimal use of deployed AMI infrastructures.
- Development of new information-sharing protocols along with associated standards
- Hastening of AMI deployments and support for emerging applications
- Technical and policy guidance on information security/privacy for increased customer participation

Expected Outcomes:

- Metrics to quantify customer privacy and define its role in an overall cyber-security context for AMI.
- Multiple privacy-preservation mechanisms resulting in enhanced cyber security.
- The design for a more resilient and effective information-sharing communications infrastructure

Potential Applications:

- Mechanisms to reassure customers about the preservation of their privacy by adopting smart meters
- Enhanced transmission and distribution grid reliability through better utilization and re-design of existing information-sharing infrastructure.
- A more efficient and economically viable communications infrastructure that better enables remote control and coordination of loads.

PSERC

Information Hierarchy in Renewable Resource Integration

Optimal Procurement, Dispatch, and Cost Allocation

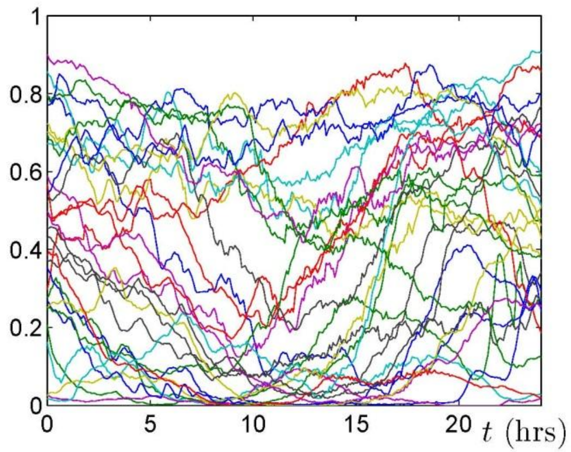
Eilyan Bitar and Lang Tong
Electrical and Computer Engineering
Cornell University

The Variability Challenge

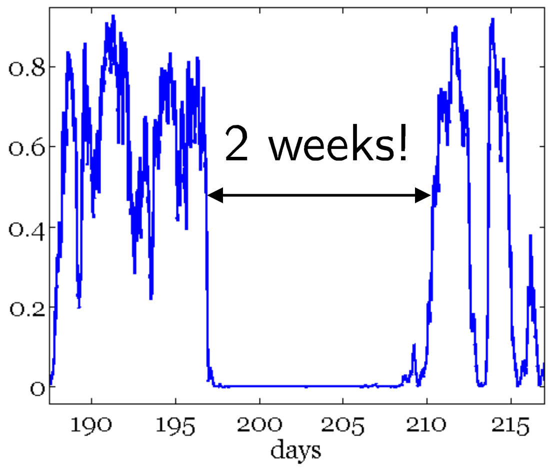
Wind and solar are variable sources of energy:

- Non-dispatchable – cannot be controlled on demand
  - Intermittent – exhibit large fluctuations
    - Uncertain – hard to forecast

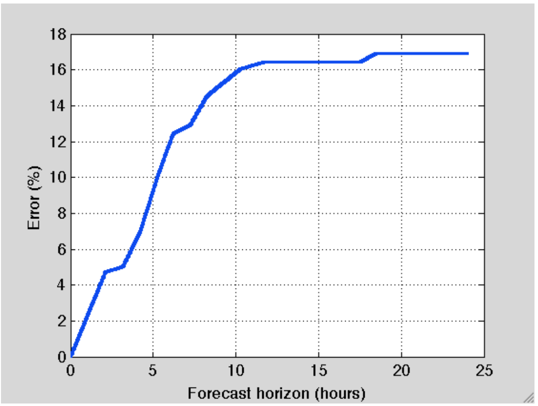
Huge variance in daily patterns



Non-stationary process



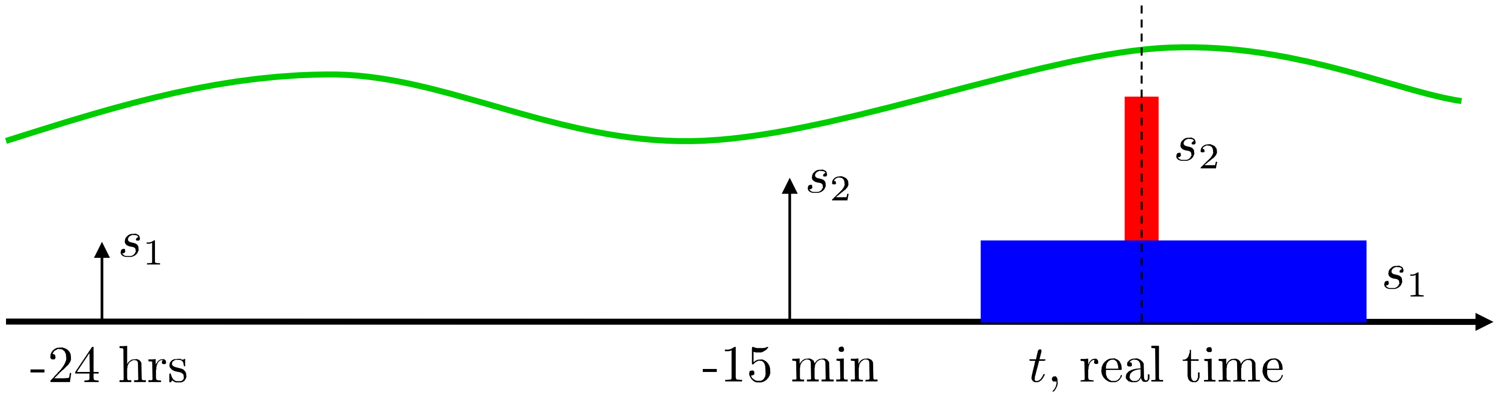
Large forecast error



Variability poses serious operational challenges for the electric grid!

Current Practice: Energy Procurement

All wind power is taken; treated as negative load $D(t) = L(t) - W(t)$



[24 hrs ahead], SO purchases 1 hour block: $s_1 = \widehat{D}(t|\text{-24 hrs})$

[15 min ahead], SO purchases 5 min block: $s_2 = \hat{D}(t| - 15\text{min}) - s_1$

[real time], SO delivers: $S(t) = s_1 + s_2$

Imbalance $= D(t) - S(t)$, covered by reserve capacity

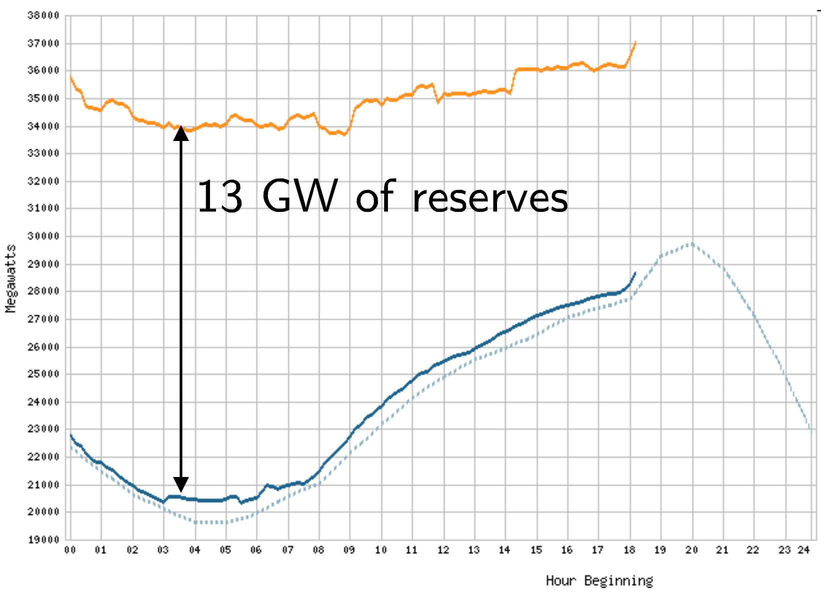
PSERC

Current Practice: Reserve Capacity Procurement

- In order to *hedge quantity risk* in net demand $D(t)$, SO purchases reserve capacity R in a forward market [call option]

$$R = \max\{7\% \text{ of } \widehat{D}(t|\text{-24 hrs}), \quad \text{largest single contingency}\}$$

EX: *CAISO*, 10/23/2011



- Reserve R dispatched in real time to match imbalances
- R insufficient to cover imbalance $D(t) - S(t) \implies$ load shedding

Shortcomings with the Current Approach

What's wrong with the current approach?

- *Certainty-equivalent* decisions
  - Treat net-load forecasts as truth when scheduling energy in sequence of forward markets
  - Do not incorporate forecast error/distribution into decision making

- *Myopic* decisions
  - Decisions decoupled across markets (ex: day-ahead, hour-ahead, real-time)
  - Here-and-now decisions do not take recourse opportunities into account

- Cost allocation not based on cost causation
  - The incremental costs of ancillary services required to compensate variability in renewables are socialized amongst the load serving entities.
  - This approach will become untenable at levels of increased penetration.

PSERC

Research Objectives

Risk Limiting Procurement and Dispatch of Reserves and Energy

-Characterize stochastic optimal control policies to co-optimize reserves + energy across a sequence of intra-day markets

-Have existing results for single-bus setting [Rajagopal et al. 2013]

-Will consider constrained transmission network setting in proposed work

Fair Cost Allocation Mechanisms: Axioms and Mechanism Design

-We transform the set of qualitative cost allocation principles in [1] into precise mathematical `fairness axioms'.

-We will identify transparent cost allocation mechanisms that can be efficiently computed – satisfying fairness axioms.

-The challenge lies in disentangling the individual elements of causation from the aggregate cost resulting from a network-wide optimization.

Stochastic Optimization in Demand Response

-We study the interactions among ISO, utility, and end-user in demand response in the presence of random uncertainties. We develop, within the framework of two settlement wholesale market, the optimal pricing policy for the utility to facilitate consumer demand response.

PSERC

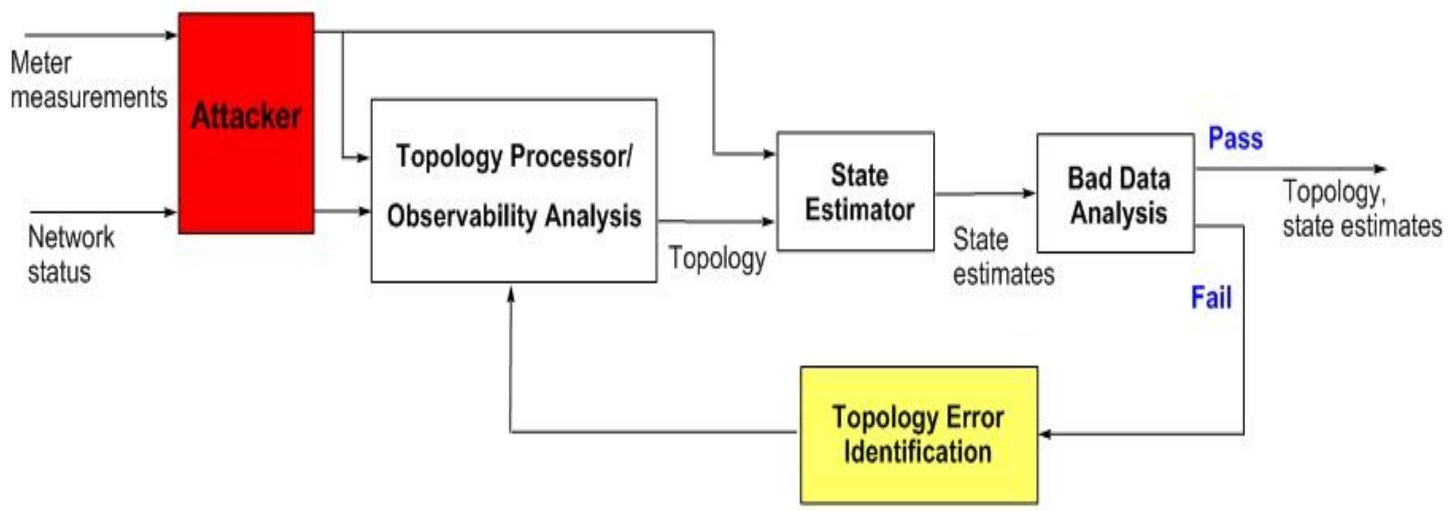
[1] D. Tretheway, "Cost allocation guiding principles" CAISO draft final proposal, March 15, 2012

Understanding and defending against cyber attack on future grid

Lang Tong and Eilyan Bitar
Cornell University, Ithaca, NY 14850

PSERC

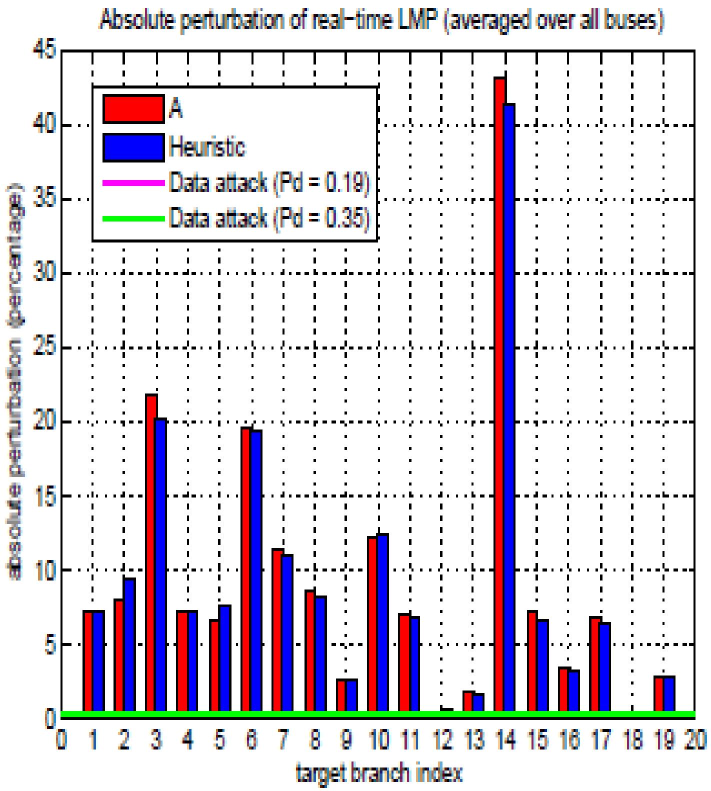
Man-in-the-middle attack

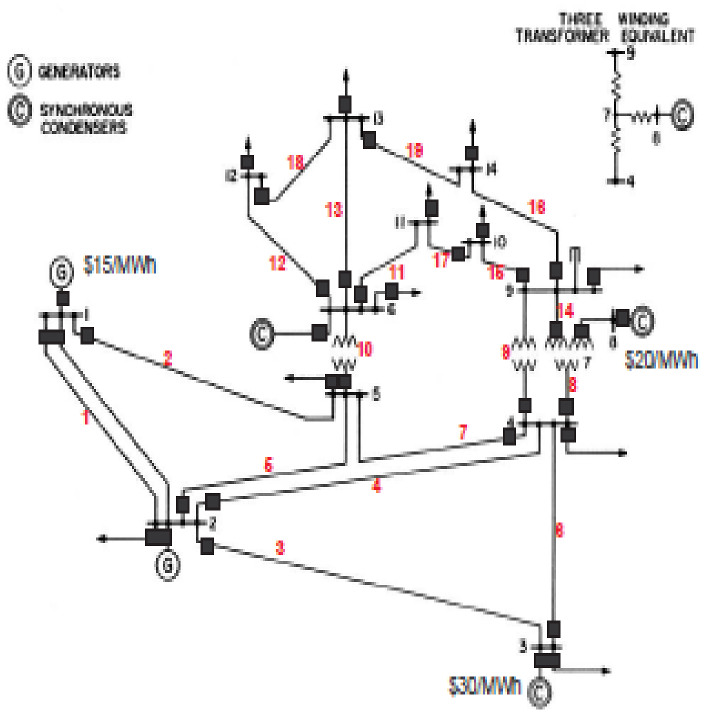


- ❑ Attacker intercepts data packets and replace it with malicious data
- ❑ If undetected, the attacker may be able to
  - ❑ mislead the control center about the topology and the state of the network;
  - ❑ mask actual contingencies or create false contingencies

PSERC

Example: topology attack

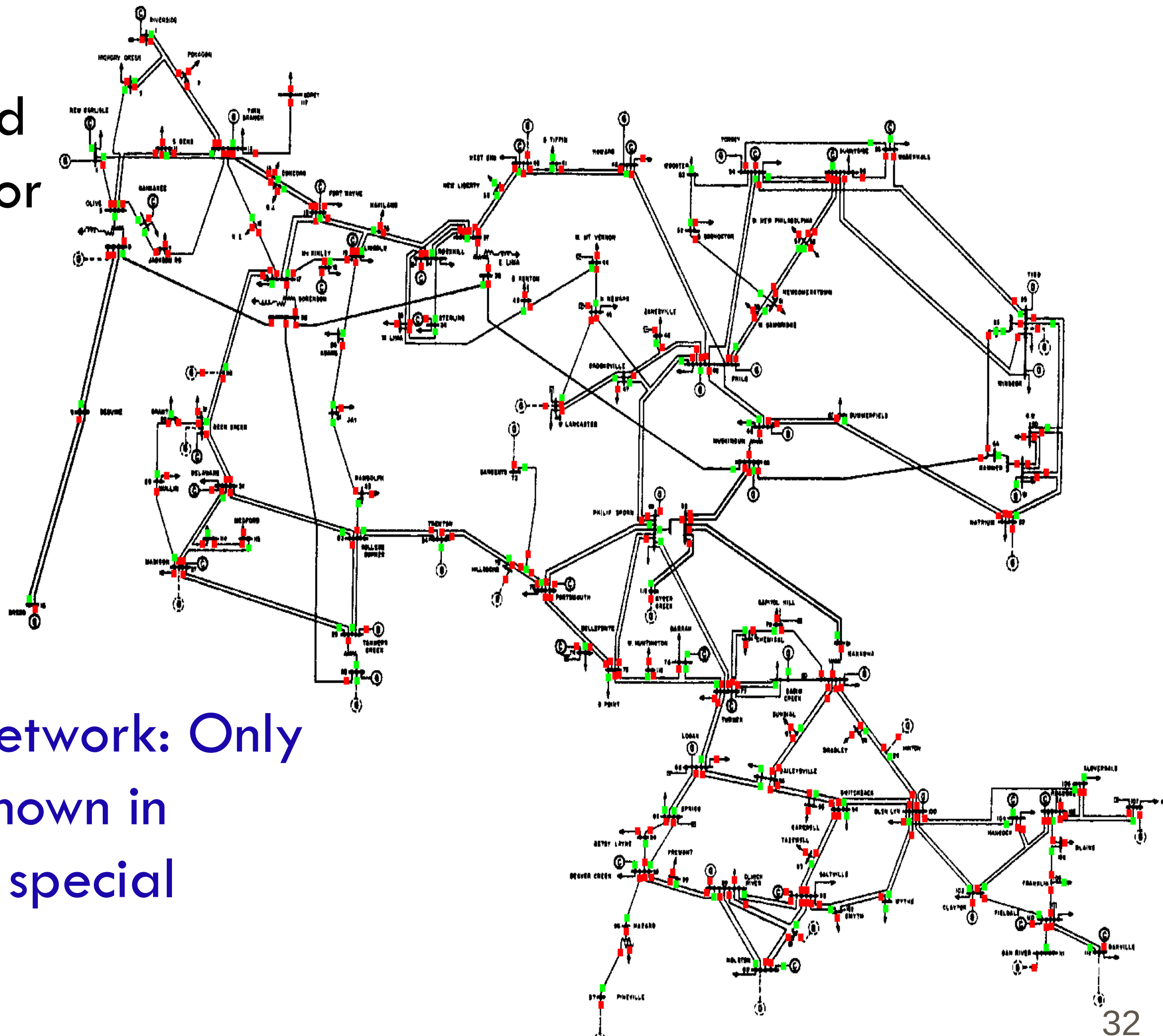




Change a few (<5) meter data and use only local information causes significant change (up to 40%) in LMP

Relevant recent results

- Obtained algebraic and topological conditions for undetectable attacks.
- Implications: making attack detectable by protecting data at key locations



IEEE 118 bus network: Only 30% meters (shown in green) require special protection

Objectives and scope

Objectives:

- ❑ Understand mechanisms of cyberattacks on control center.
- ❑ Quantify potential impacts of different forms of attacks
- ❑ Develop defense mechanisms against attacks

Scope:

- ❑ Develop realistic models of attack on sensors and substations
- ❑ Characterizing impacts of attack on state estimation and dispatch
- ❑ Develop intrusion and malicious data detection techniques
- ❑ Develop protection and prevention mechanisms