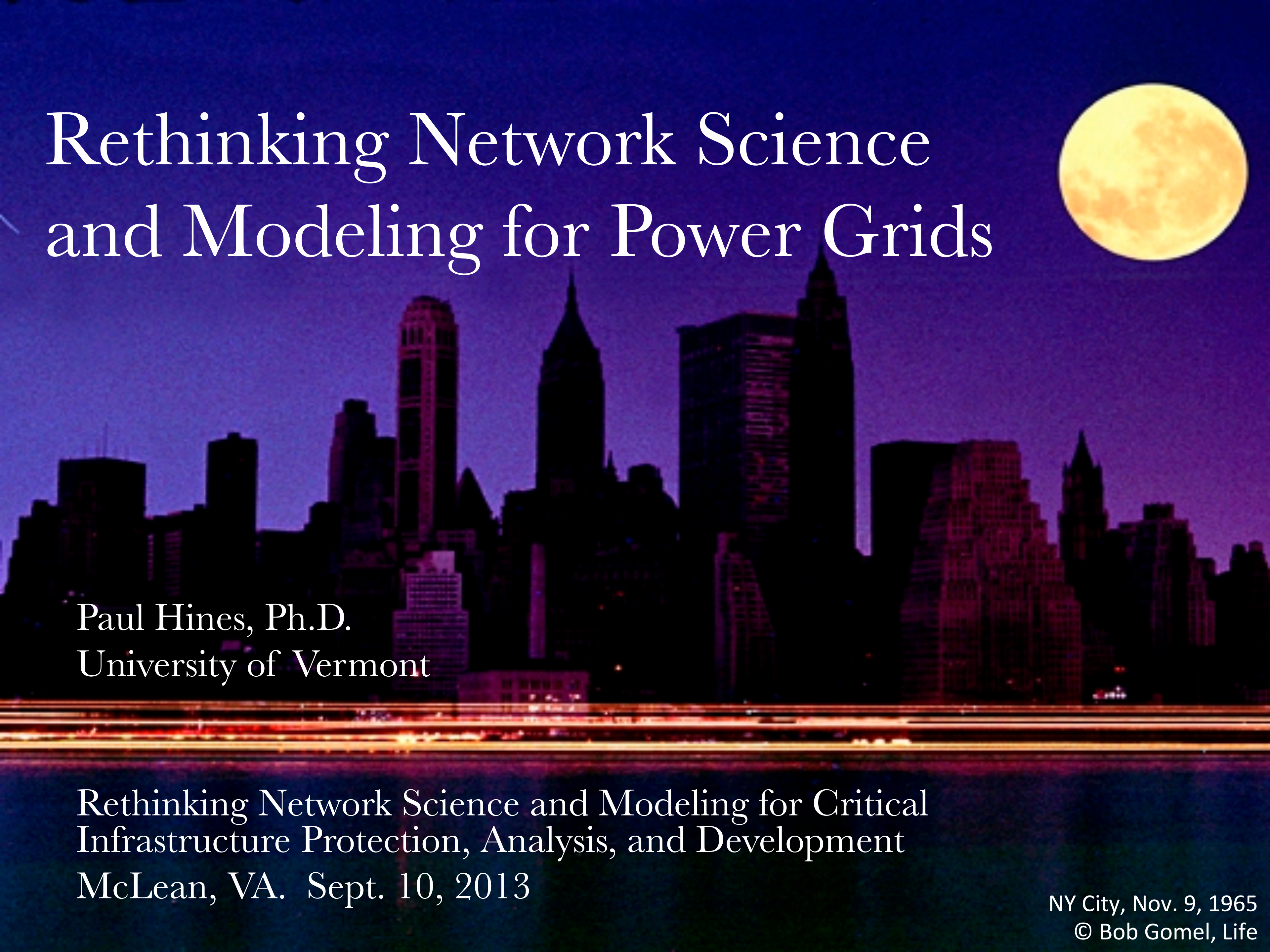
Rethinking Network Science and Modeling for Power Grids

Paul Hines, Ph.D.
University of Vermont

Rethinking Network Science and Modeling for Critical Infrastructure Protection, Analysis, and Development
McLean, VA. Sept. 10, 2013



NY City, Nov. 9, 1965

The power grid is an important challenge

- $371 billion in sales in 2011, United States
- Annual cost of power outages: $20-$100 billion
  - LaCommare & Eto, *Energy*, 2006
- The only way to move almost any type of energy (e.g., renewables), to billions of homes, almost instantly

Hines, Sep. 2013

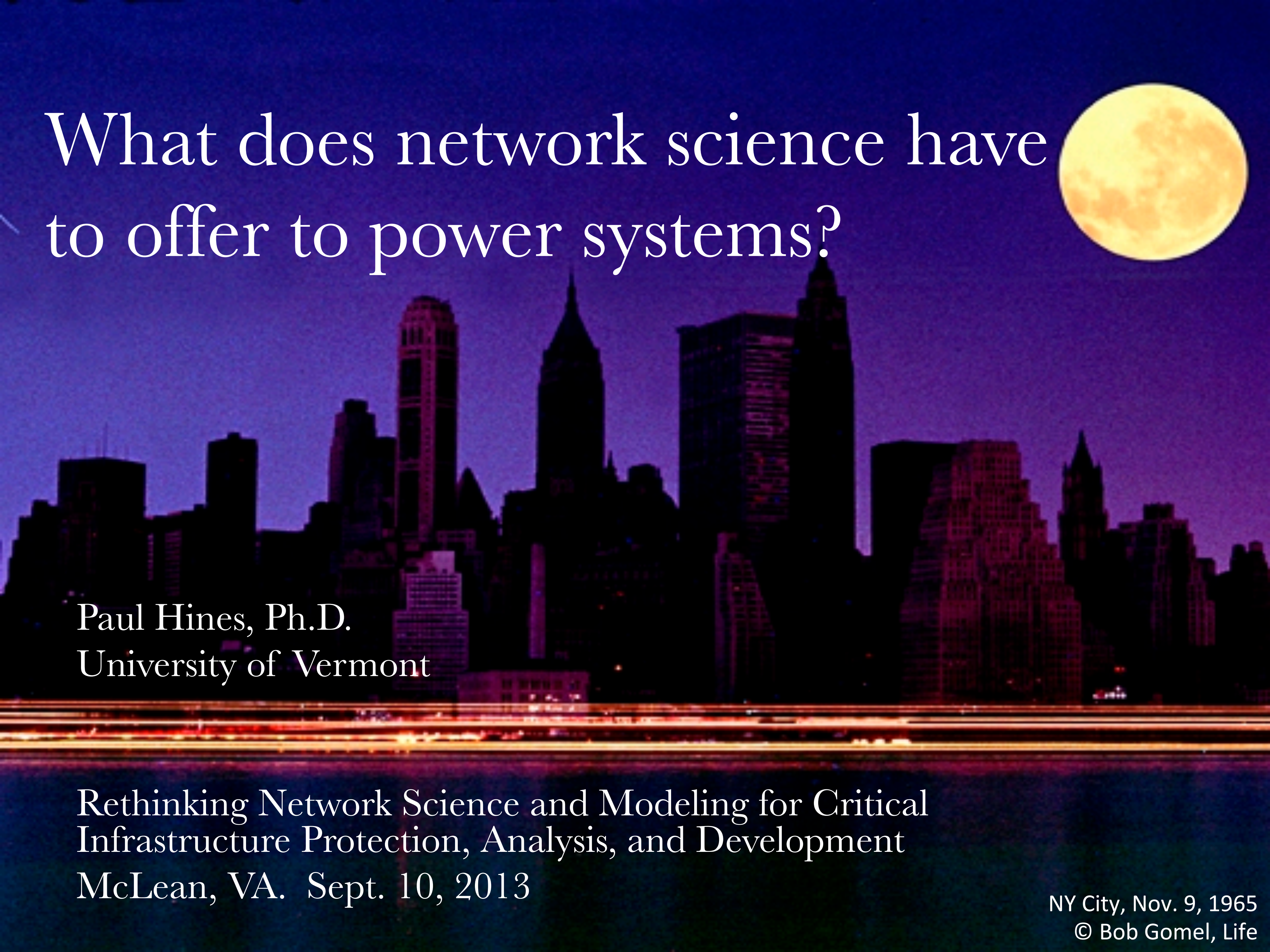
Outline

- What does network science have to offer to power systems?
- What does power systems have to offer to network science?
- What can we learn by comparing models?
- What can we do to bring these two fields together?

What does network science have to offer to power systems?

Paul Hines, Ph.D.
University of Vermont

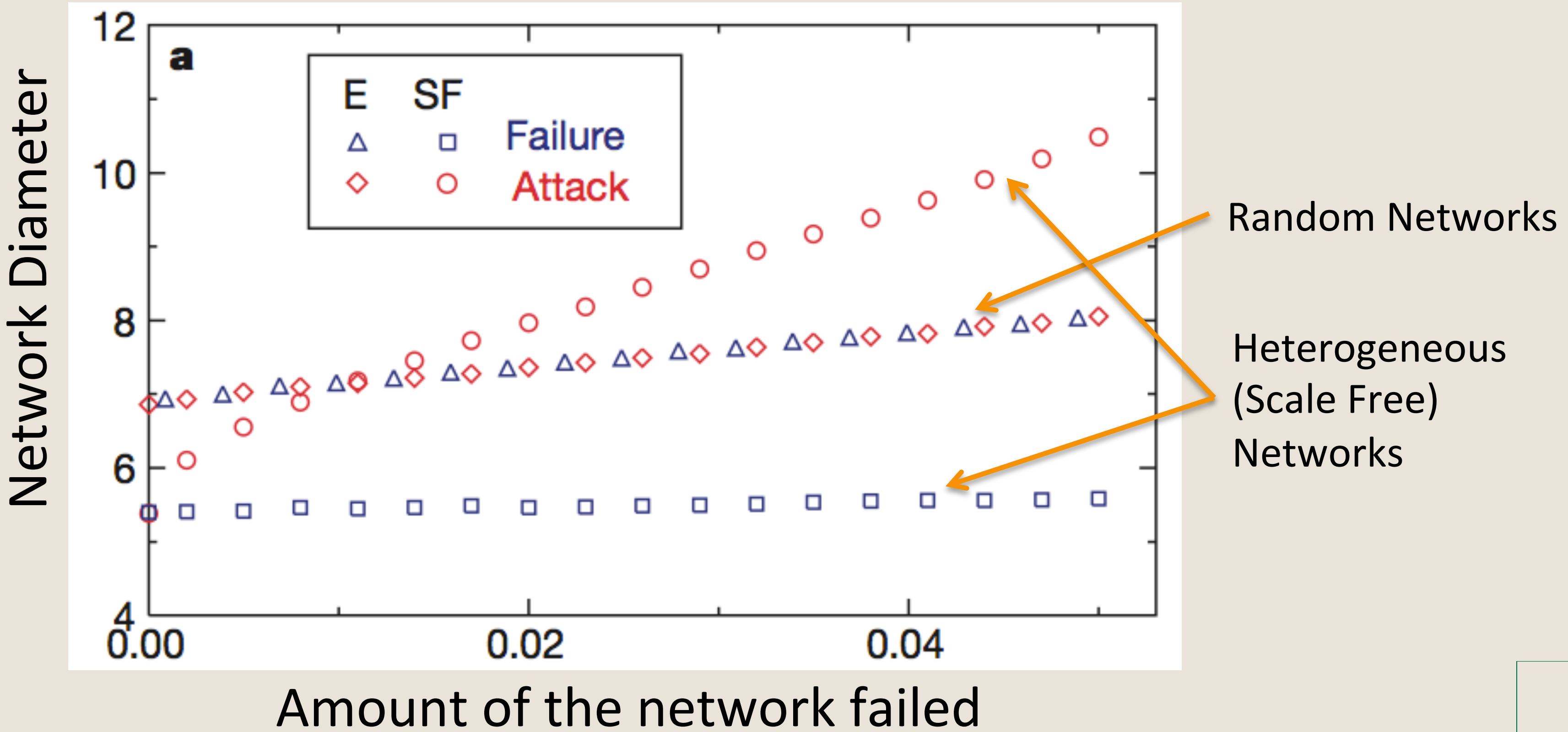
Rethinking Network Science and Modeling for Critical Infrastructure Protection, Analysis, and Development
McLean, VA. Sept. 10, 2013



NY City, Nov. 9, 1965

What does network science have to offer?

- New ways of thinking about vulnerability
  - Albert, Jeong, Barabasi, “Error and Attack Tolerance of Complex Networks,” *Nature*, 2000



What does network science have to offer?

- Illustrating the value of simple models

Toy models
Easy to understand
Quickly provide "insight"
Might be misleading

"Flight Simulator" engineering models.
Many parameters.
Potentially more accurate.
Outputs can be hard to understand.

Model "complicatedness"

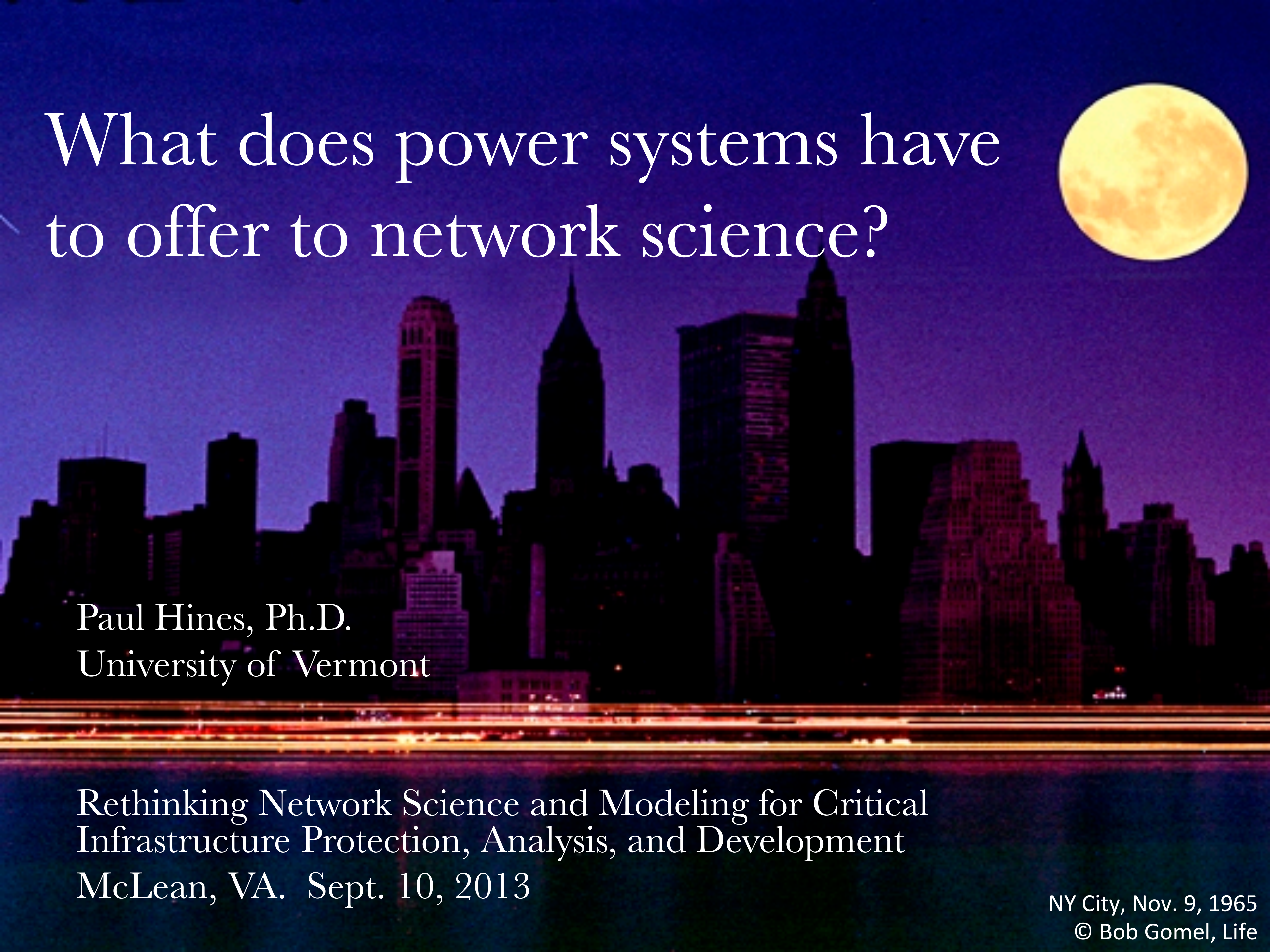
Rarely, do we carefully consider the humans in our infrastructure models---even (especially) the very complicated ones.

What does power systems have to offer to network science?

Paul Hines, Ph.D.
University of Vermont

Rethinking Network Science and Modeling for Critical Infrastructure Protection, Analysis, and Development

McLean, VA. Sept. 10, 2013

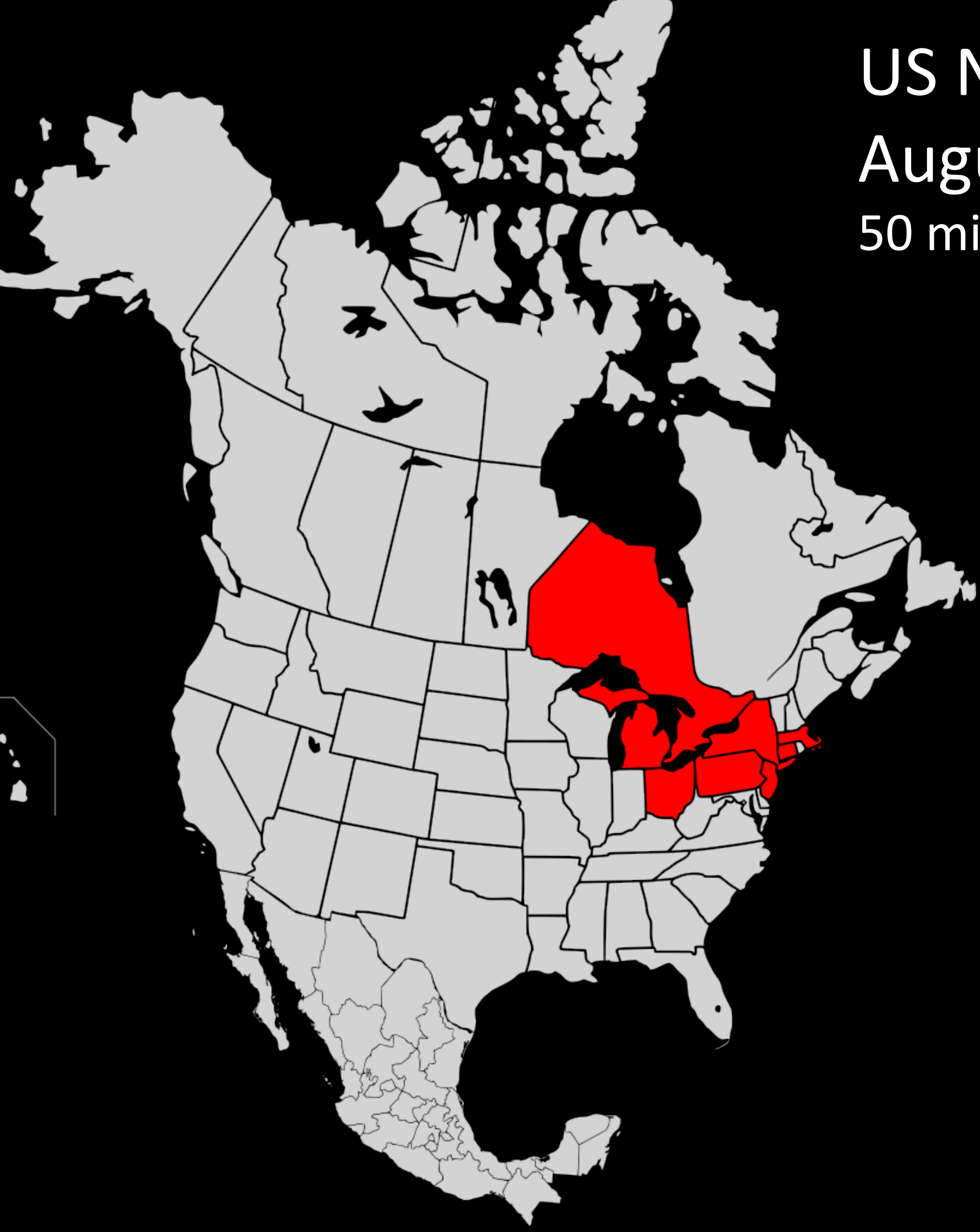


NY City, Nov. 9, 1965

1. A challenging problem

- Nov. 9, 1965
  - 30 million people affected!
- July 13, 1977
  - Widespread looting, chaos. >3000 arrests.
- Italy, 2003
  - Several deaths (traffic lights & falls)
  - Thousands stranded in transit
- Germany/France, Nov. 2006
  - >15 million affected
  - “Europe came very close to a complete blackout.” –Bornard
- Brazil, Nov. 2009
  - 50 million w/o power

US Northeast and Canada
August 14, 2003
50 million people



California, Arizona, Mexico
September 8, 2011
5 million people

Hines, Sep. 2013

Northern India

July 30, 2012: 350 million people

July 31, 2012: 700 million people

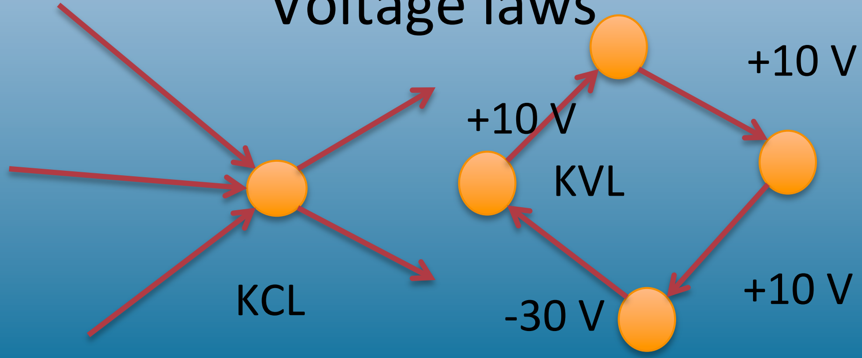
Photo: Bikas Das/AP Photo
IEEE Spectrum, Oct. 2012

Cascading failure is challenging because

- Continuous and discrete dynamics
- Enormous uncertainty
- Many mechanisms
  - Cascading overloads
  - Voltage collapse
  - Wild generator oscillations
  - Motors stalling
  - Operator errors
- Several competing (complementary) models
  - No "established models"
    - (However some models make more sense than others)

2. Some known physics

Kirchhoff's Current and Voltage laws



Ohm's law

$$V = IR$$

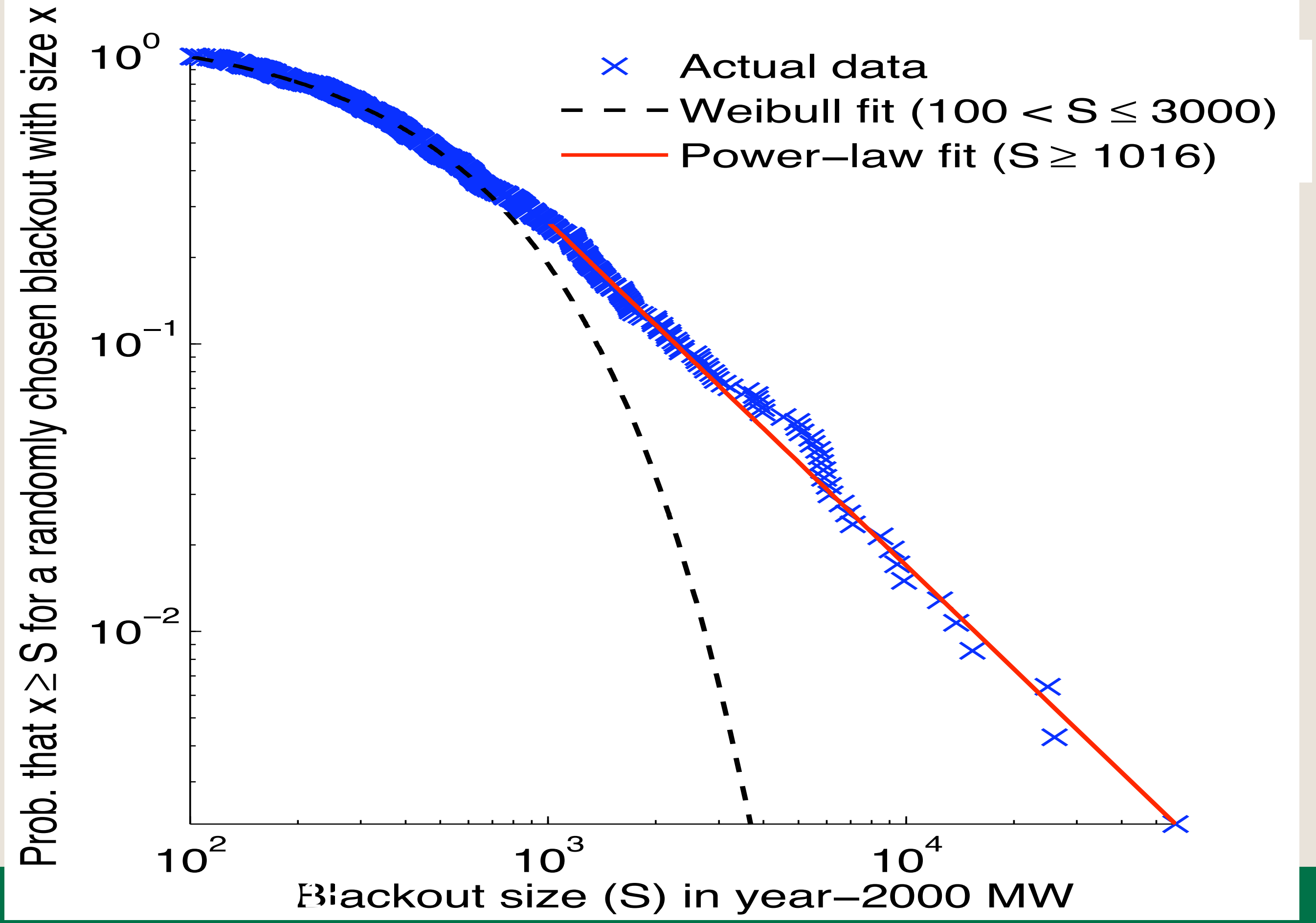
3. Some data and models to start with

- Several publically available test networks to work with
  - Cascading is a “large-scale” problem. Use larger networks, such as the Polish network (MATPOWER)
- Cascading modeling details are publicly documented for
  - OPA (Dobson, Carreras, Newman)
  - CFS/DCSIMSEP (Hines)
    - Source code soon to be posted online
  - Manchester model (Kirschen)
- An increasing amount of real data is public
  - Load and market data from System Operators (e.g. ISO New England)
  - BPA wind and T-line outage data
- Other data is out there (e.g. PMUs), but much harder to obtain

4. Interesting statistical properties to explain

Power Systems have fascinating power laws

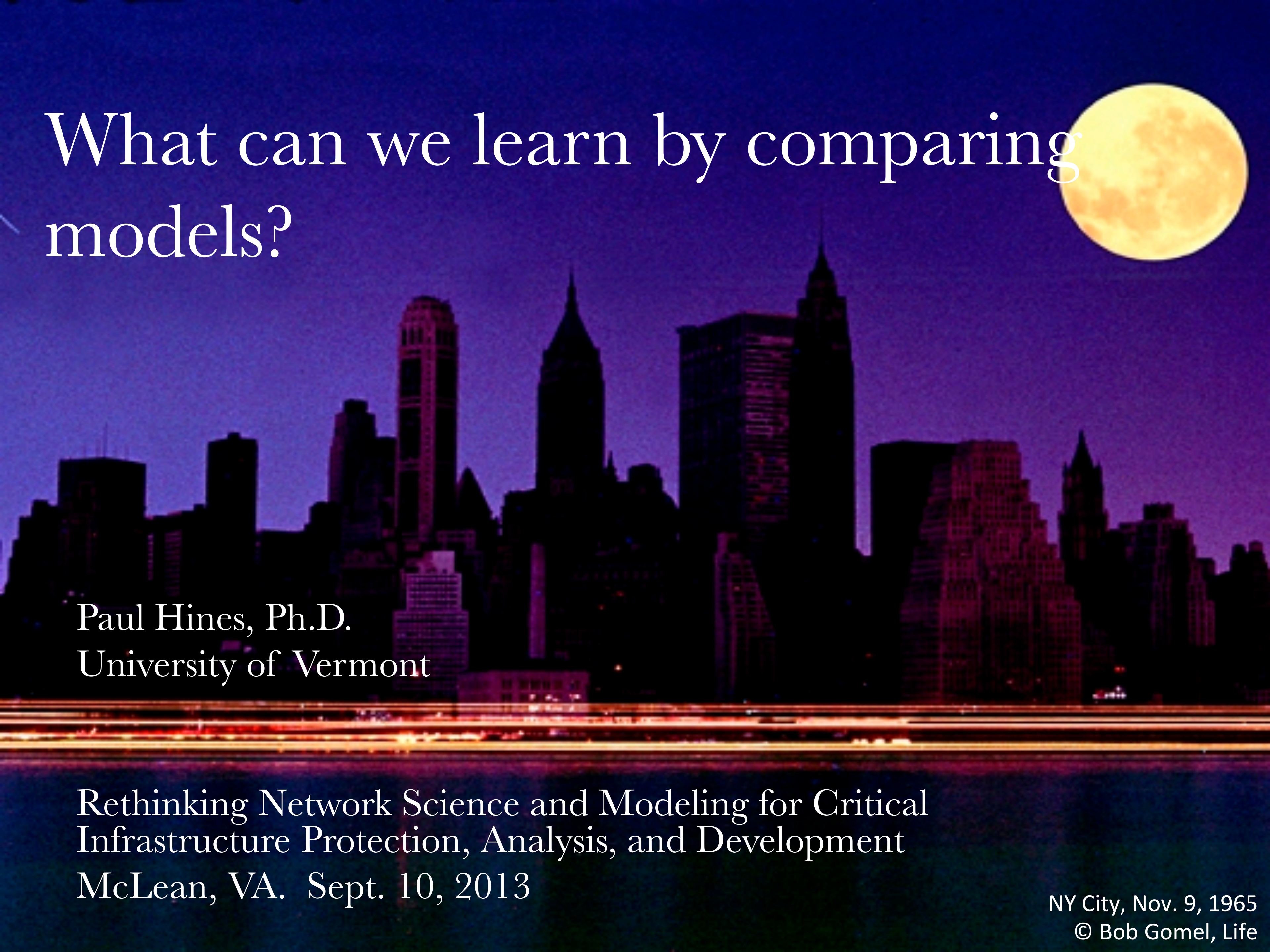
(or at least very fat tailed distributions)



What can we learn by comparing models?

Paul Hines, Ph.D.
University of Vermont

Rethinking Network Science and Modeling for Critical Infrastructure Protection, Analysis, and Development
McLean, VA. Sept. 10, 2013



NY City, Nov. 9, 1965
© Bob Gomel, Life

Methods of validation for new models

- (Dobson has also discussed)
- Optimally
  - Compare models to real data
  - Models should at least statistically match real data, for the decision of interest
- Less-optimally
  - Check for internal validity
    - Does the model make sense with respect to the known behavior of the system?
  - Cross-validity
    - Does the model have properties that are statistically similar (for the decision of interest) to established models?

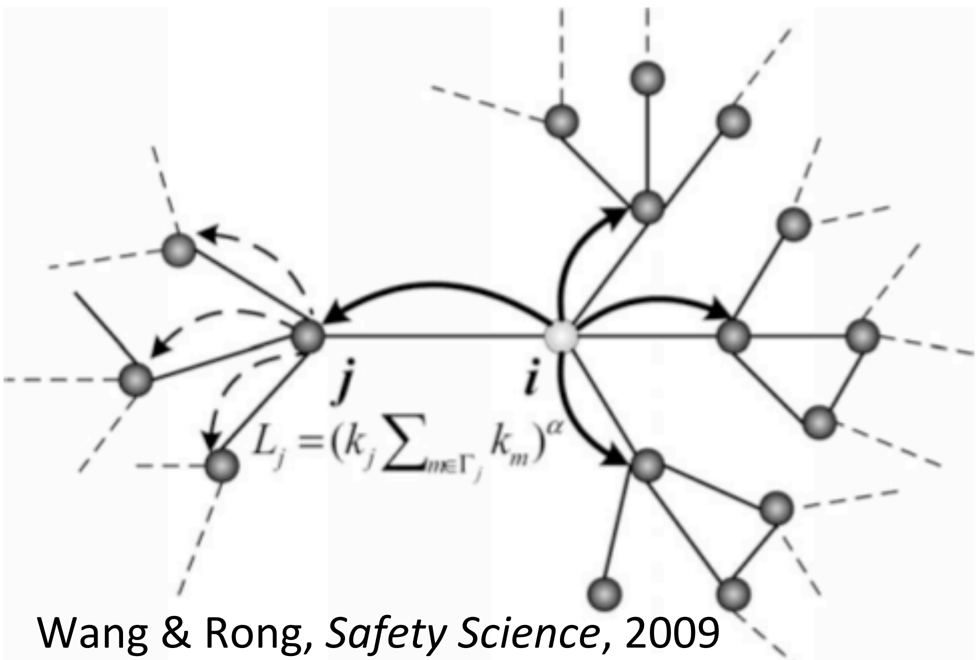
Are power grids (bizarrely) vulnerable to attacks in other ways?

The New York Times

Asia Pacific

WORLD U.S.

Academic Paper in China Sets Off Alarms in U.S.

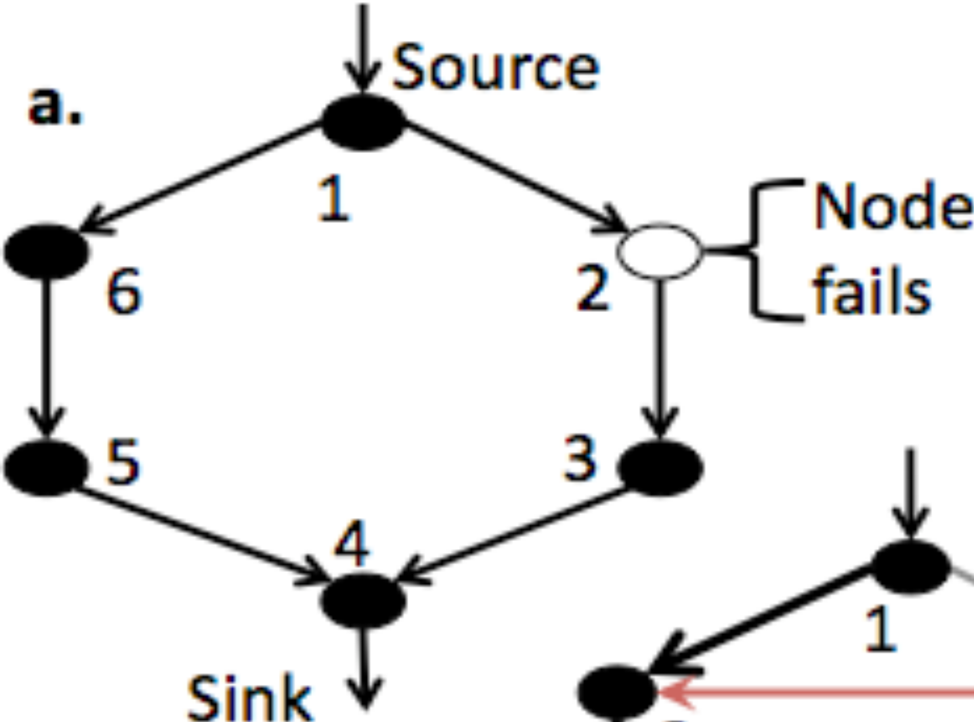


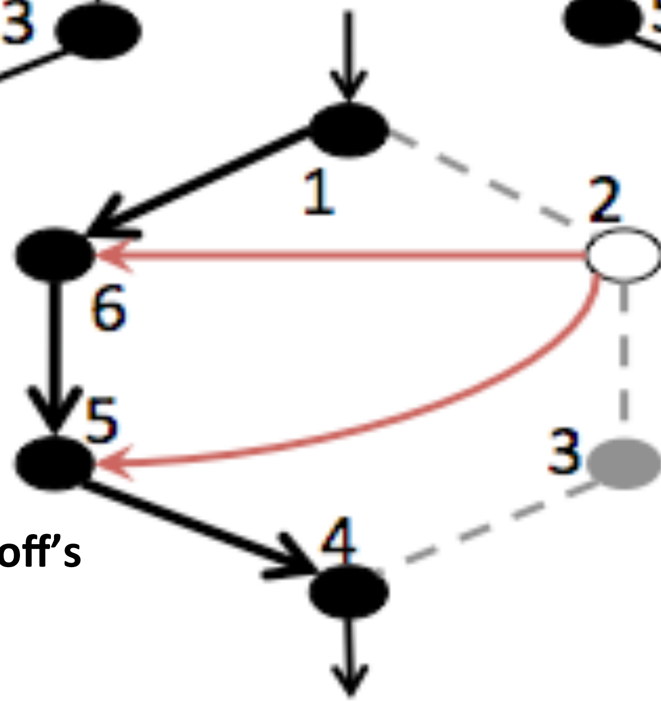
Wang & Rong, *Safety Science*, 2009

Fig. 2. The scheme illustrates the load redistribution triggered by an node-based attack. Node *i* is removed and the load on it is redistributed to the neighboring nodes connecting to node *i*. Among these neighboring nodes, the one with the higher load will receive the higher shared load from the broken node.

<u>Conclusion</u>:
If the nodes with the lowest "traffic" (power flowing through) fail (are attacked) very large blackouts will result.

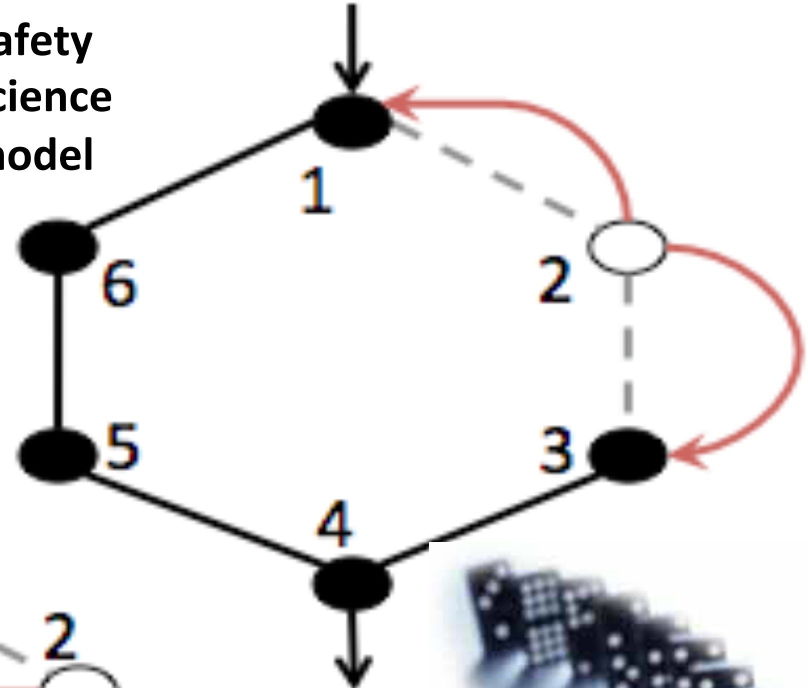
Cascades in power grids are different than "domino models"



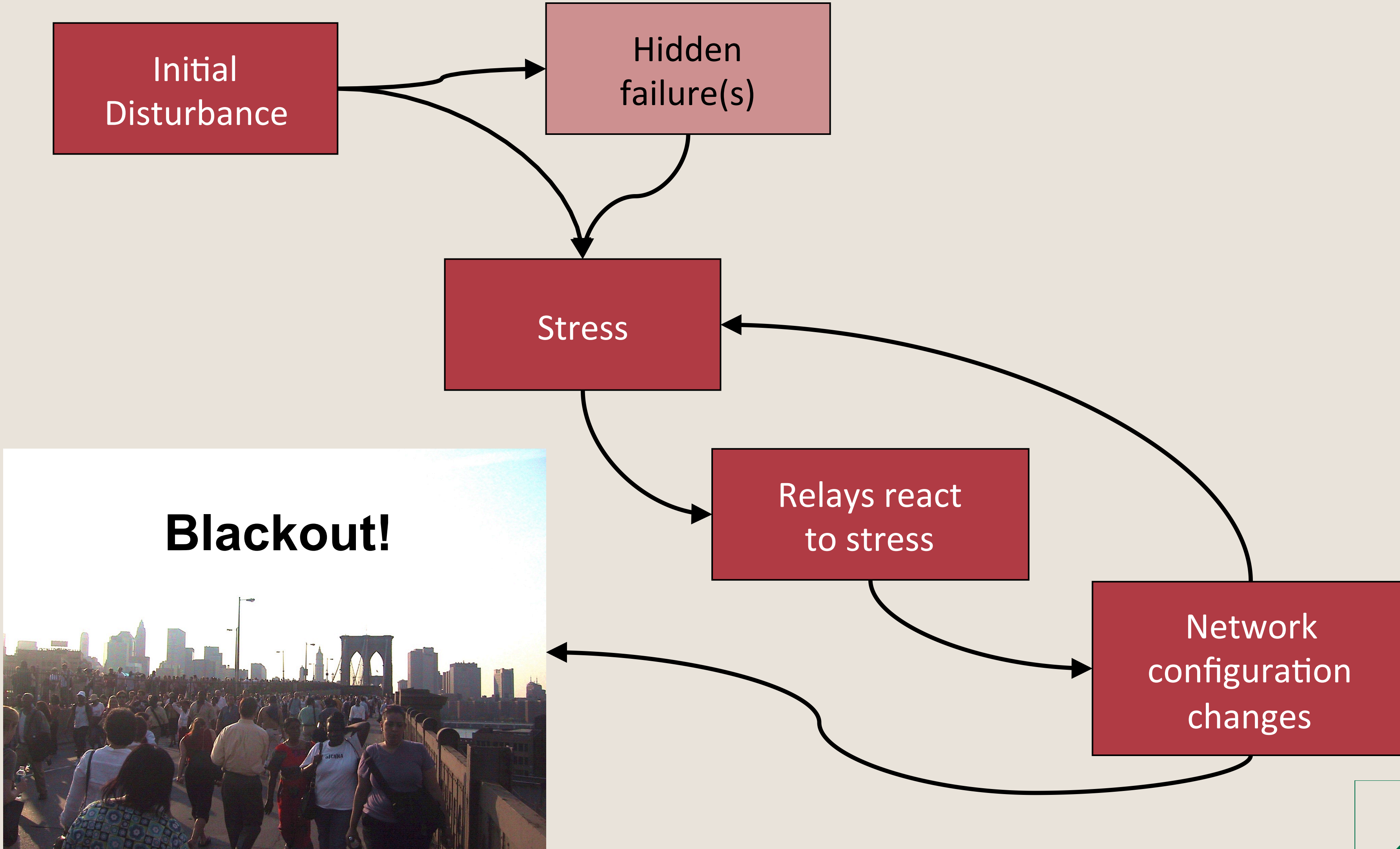


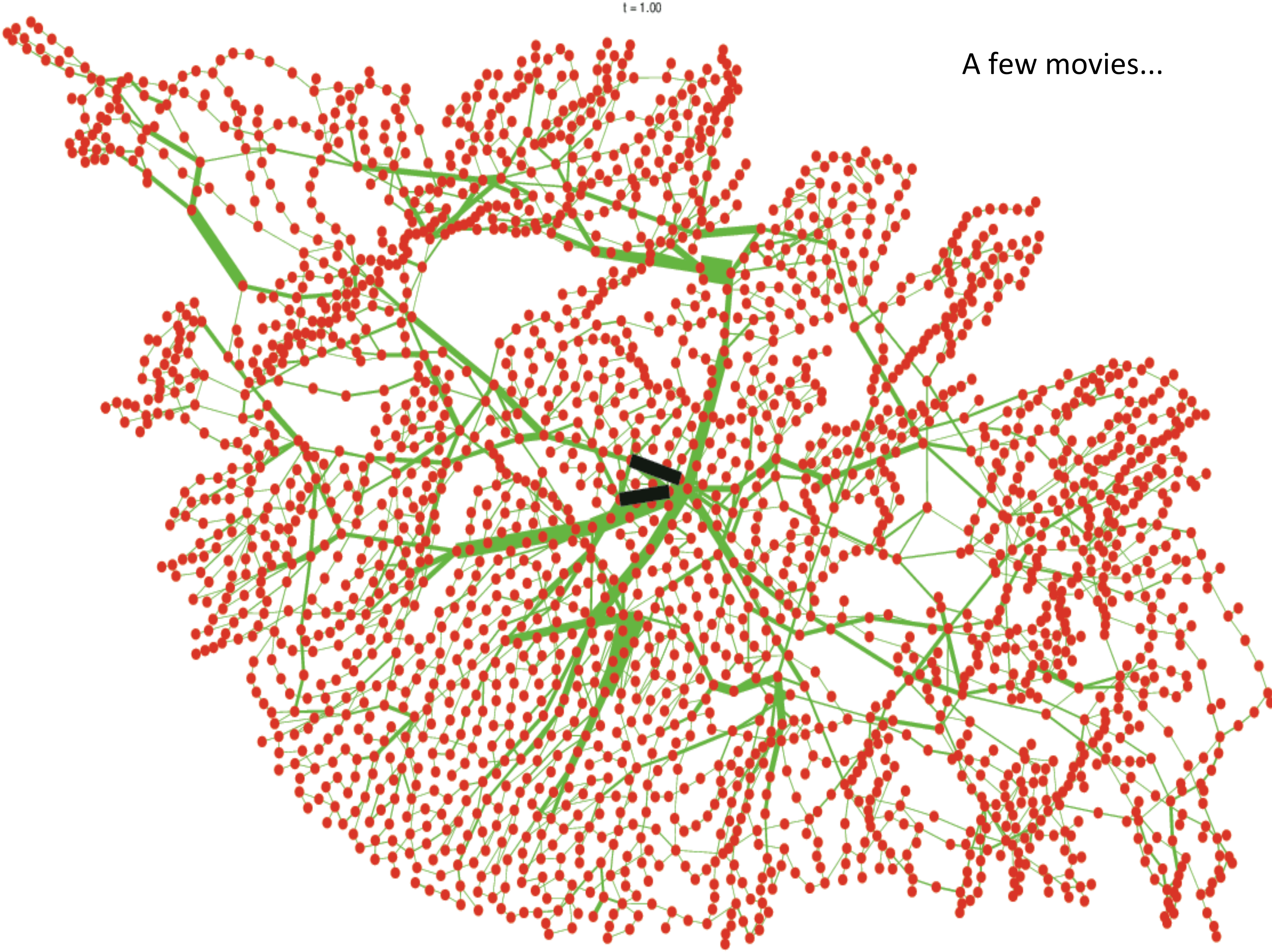
By Kirchhoff's laws

Safety science model



How cascades in power systems work

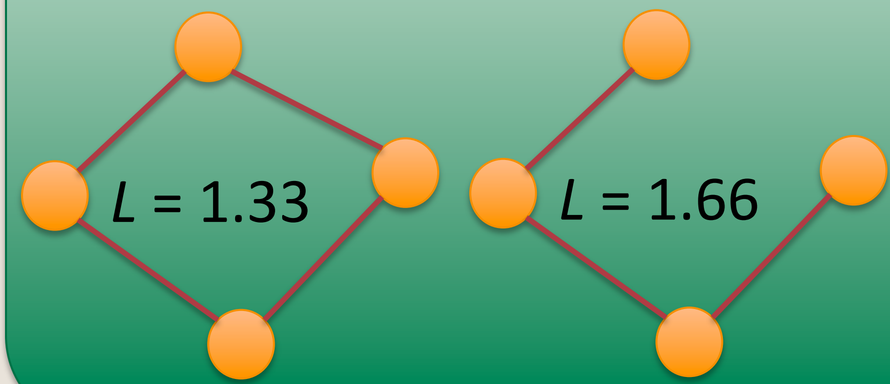




A few movies...

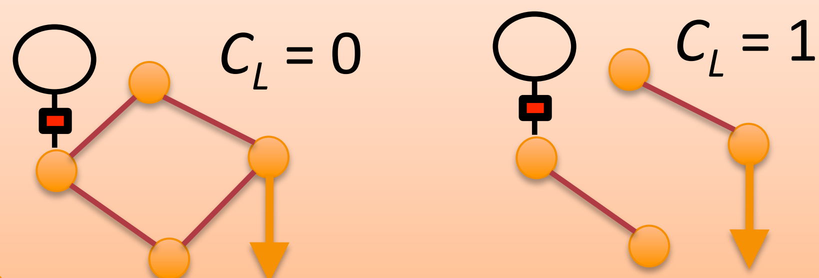
Let's run a horse race...

Characteristic Path Length

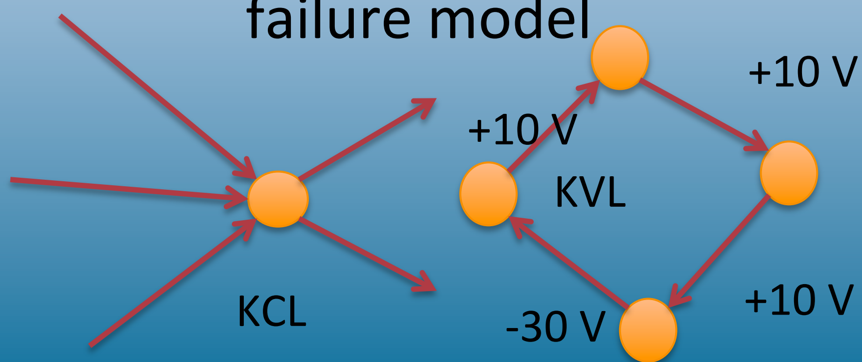


Albert et al. (2001): L increases rapidly with directed attacks in scale-free graphs, but not in random graphs

Connectivity Loss



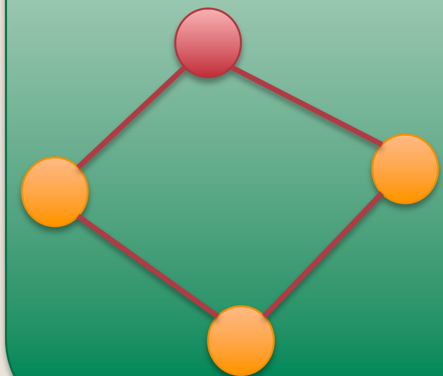
Blackout size from a cascading failure model



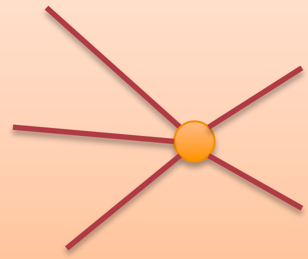
Albert et al. (2004): C_L increases rapidly as hub nodes are removed from a power grid

Attack/Failure Vectors

Random failure

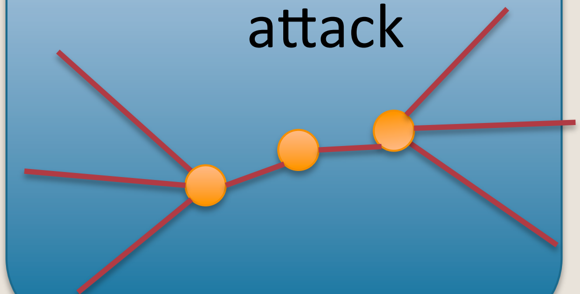


Degree-based attack



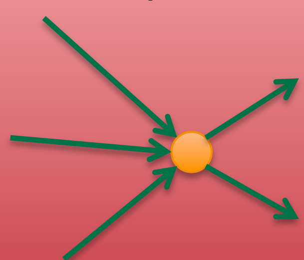
Albert et al (2000)

Betweenness attack



Albert et al (2004)

Min/max load/traffic

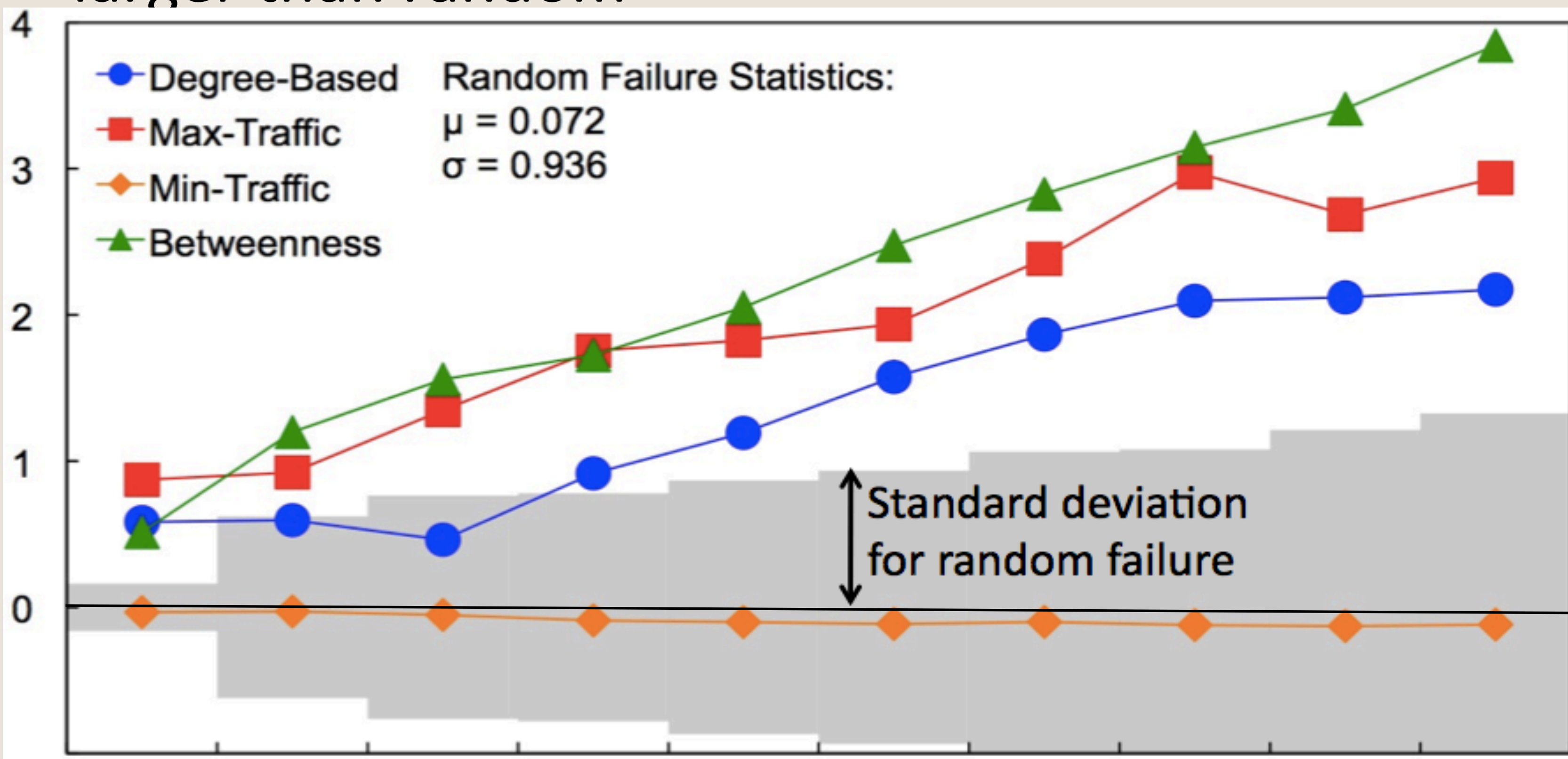


Wang & Rong (2009): Min-traffic leads to large failures

Results: Critical Path Length

High betweenness attacks are the most "successful" Min-traffic is least. Directed attacks ~2 sigma larger than random

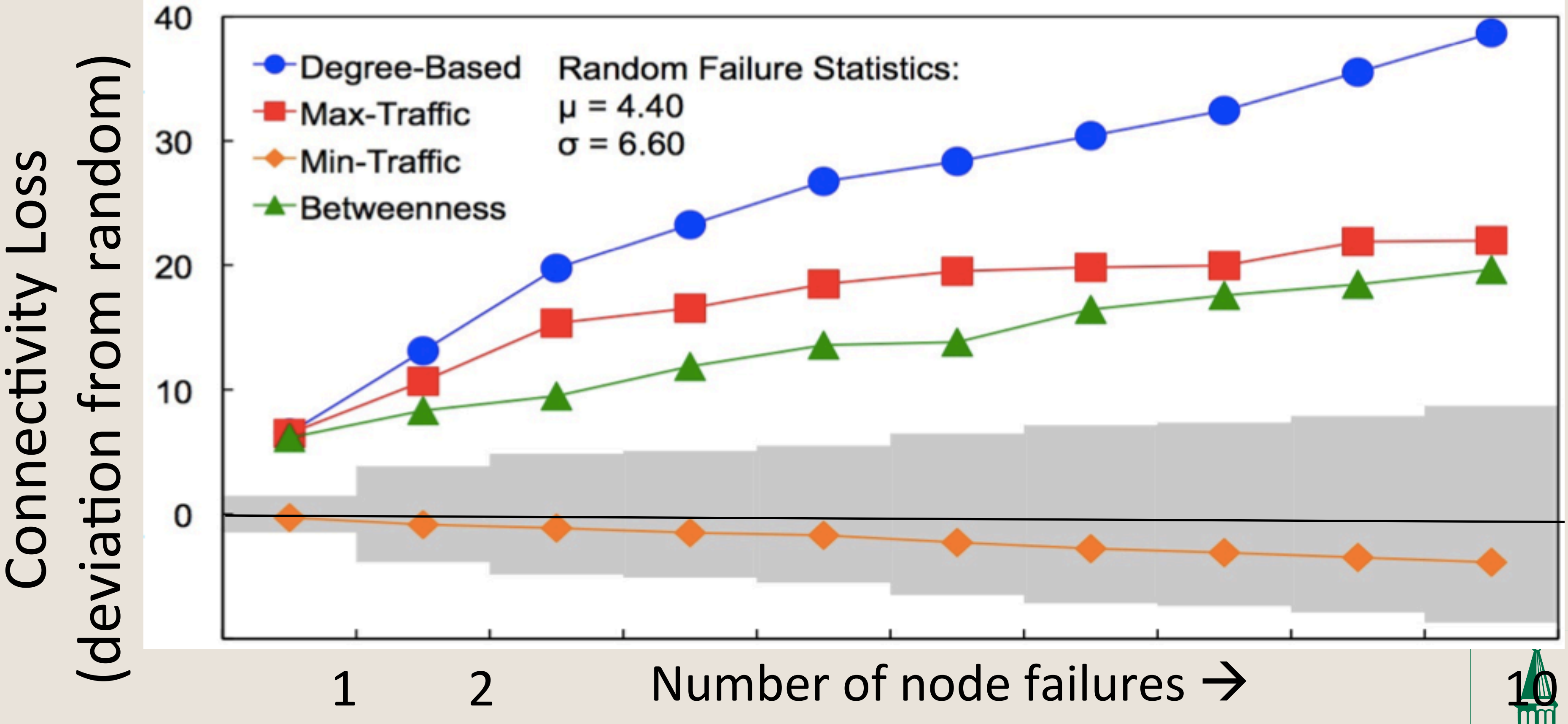
Critical Path Length (L)
(deviation from random)



1 2 Number of node failures → 10

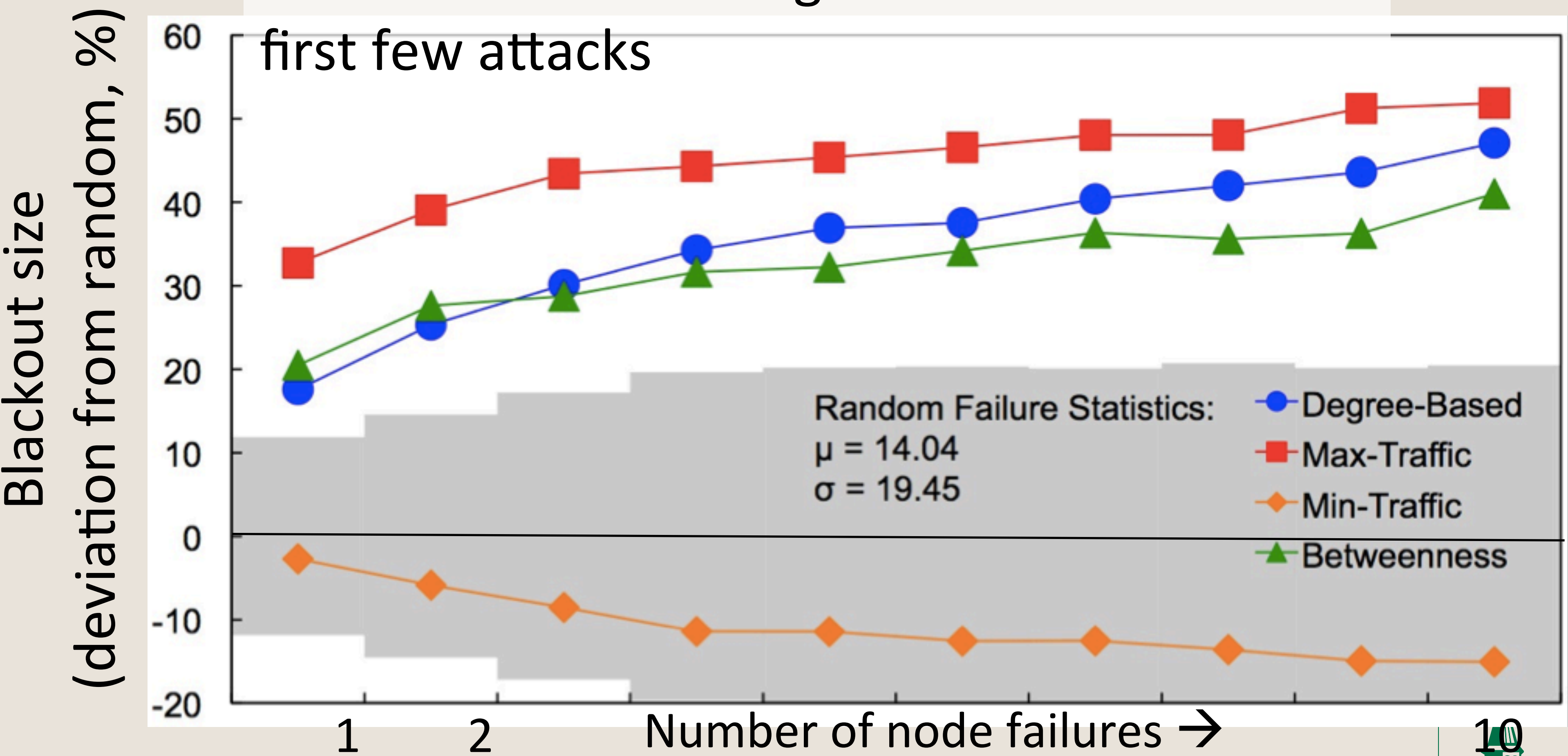
Results: Connectivity Loss

Degree-based attacks are much more "successful" Min-traffic is least. Directed attacks ~3 sigma larger than random



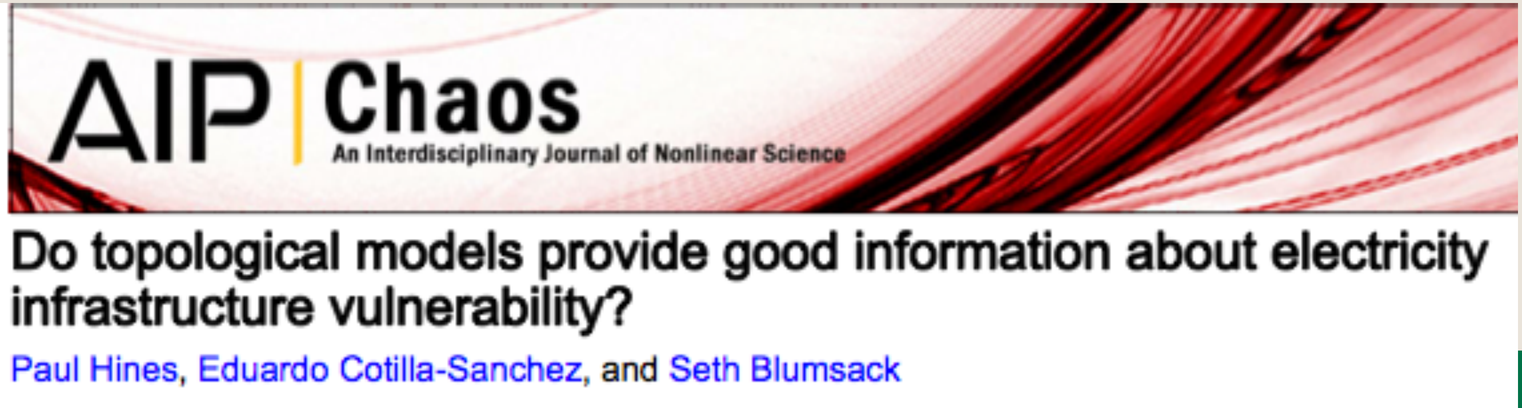
Results: Blackout Size

Max-traffic attacks are most “successful”
Min-traffic is least. Big blackouts result from first few attacks



Bottom line

- (at least some) Graph theoretic models can be ***very misleading*** in what they tell us about the response of the grid to attacks and random failures.
- Vulnerability is hard to predict. ***In general*** (but not always) the greatest vulnerabilities are ***generally*** where the power flow is greatest.


AIP | Chaos

An Interdisciplinary Journal of Nonlinear Science

Do topological models provide good information about electricity infrastructure vulnerability?

Paul Hines, Eduardo Cotilla-Sanchez, and Seth Blumsack

What can we do to bring these two fields together?

Paul Hines, Ph.D.
University of Vermont

Rethinking Network Science and Modeling for Critical Infrastructure Protection, Analysis, and Development
McLean, VA. Sept. 10, 2013

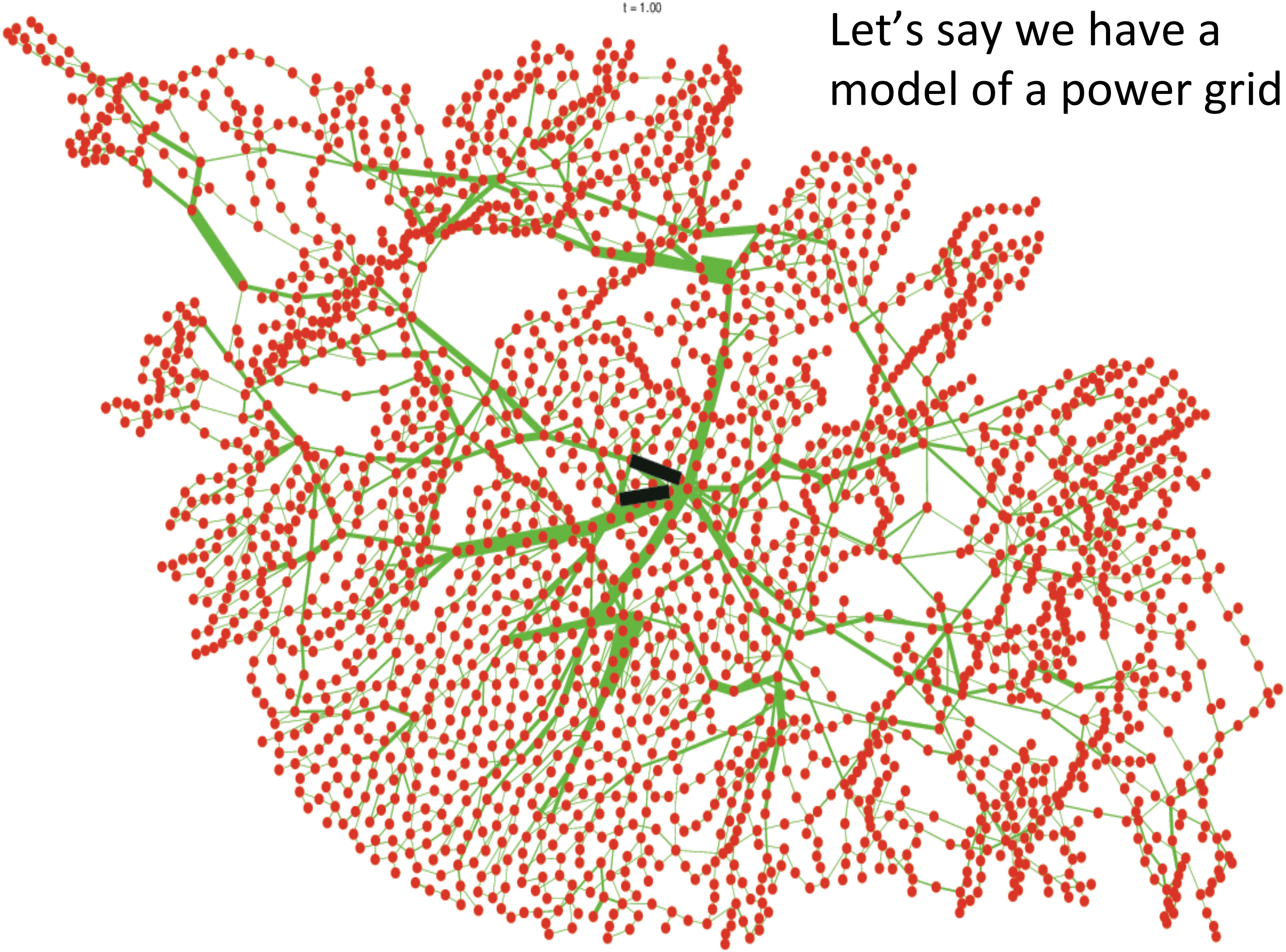
NY City, Nov. 9, 1965

What we know so far

- Simple models (such as graphs) often provide very useful insight
  - Far better to have a simple model that can produce some insight, than an engineering model that is too complicated (too many inputs) to use

- Can we combine simple models and engineering models in useful ways?

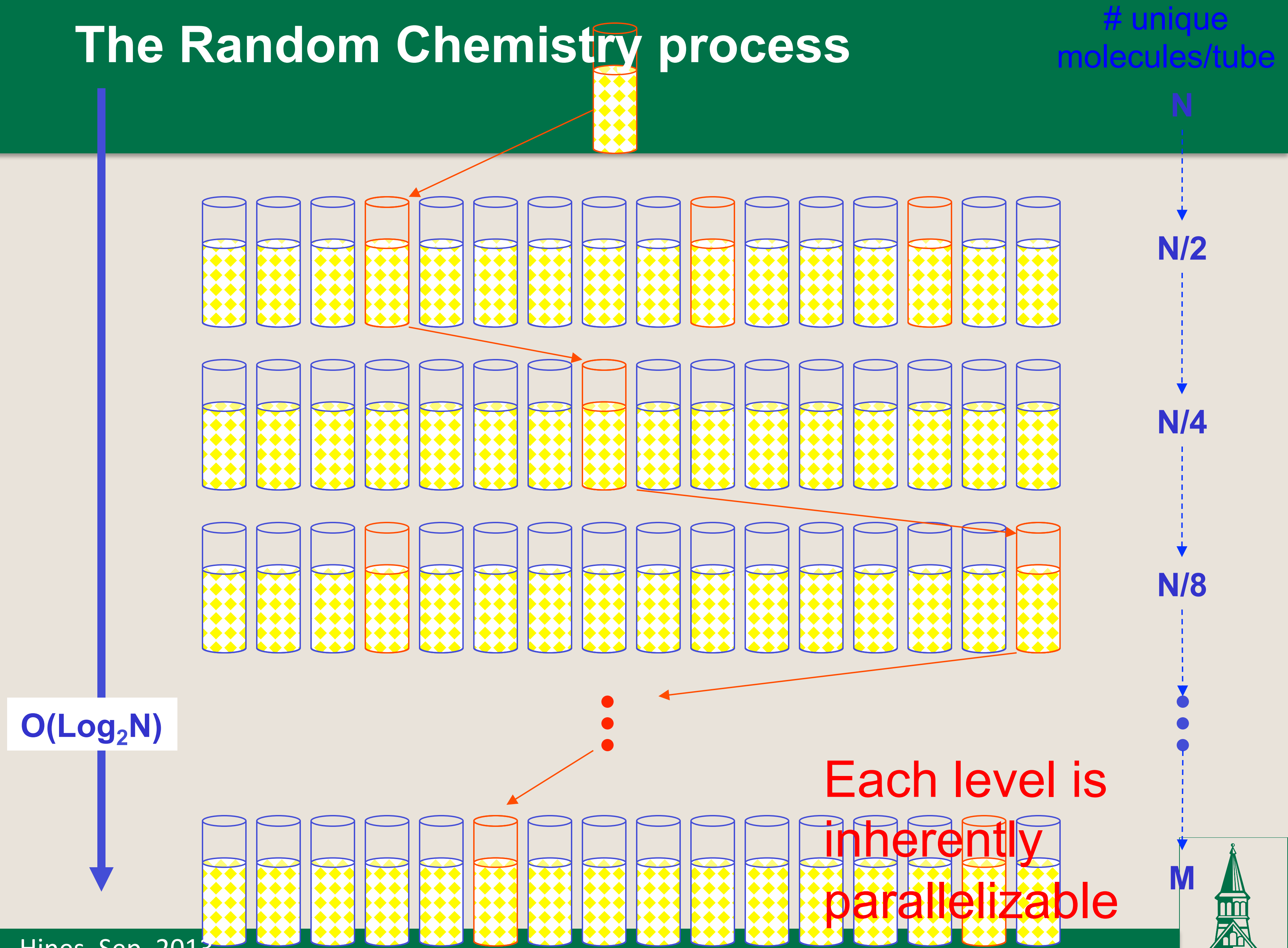
Let's say we have a model of a power grid



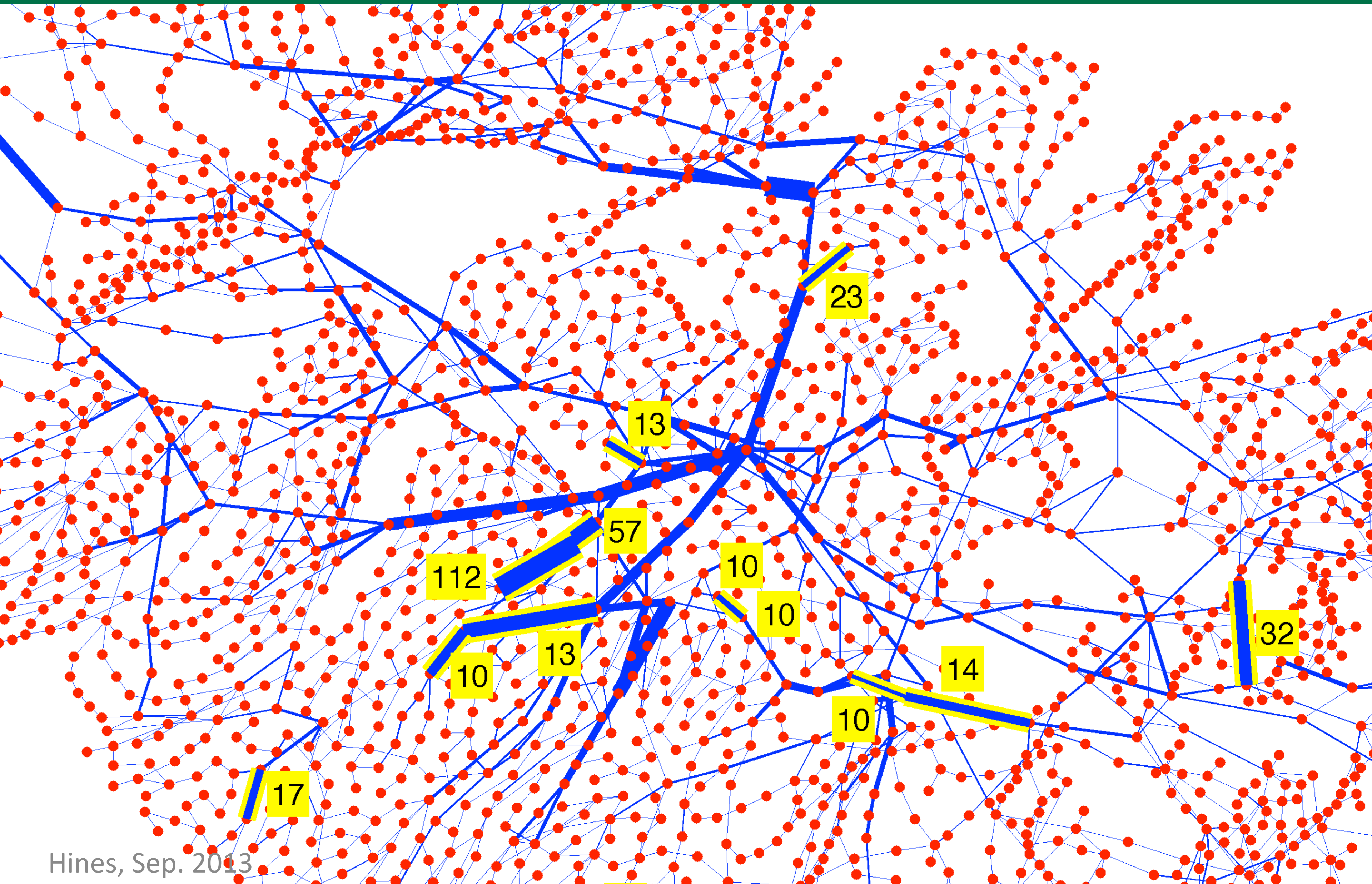
How do we find outage combinations that trigger large blackouts?

- Power system operators run thousands of calculations to make sure that the grid is "n-1" secure.
  - However, we know almost nothing about "n-k" security
- Option 1: random search (Monte Carlo)
  - Advantage: unbiased
  - Disadvantage: 12,476 simulations to find each n-2 combination
  - Disadvantage: ~150,000 simulations to find each n-3
- Option 2: Biased search (importance sampling)
  - Use information (line flows) to bias the search.
  - Disadvantages: Outcomes will be biased
- Option 3: Random Chemistry
  - Unbiased outcome within a given n-k (given k)
  - 151 simulations to find each n-2
  - 251 simulations to find each n-3
  - 471 simulations to find each n-4

The Random Chemistry process

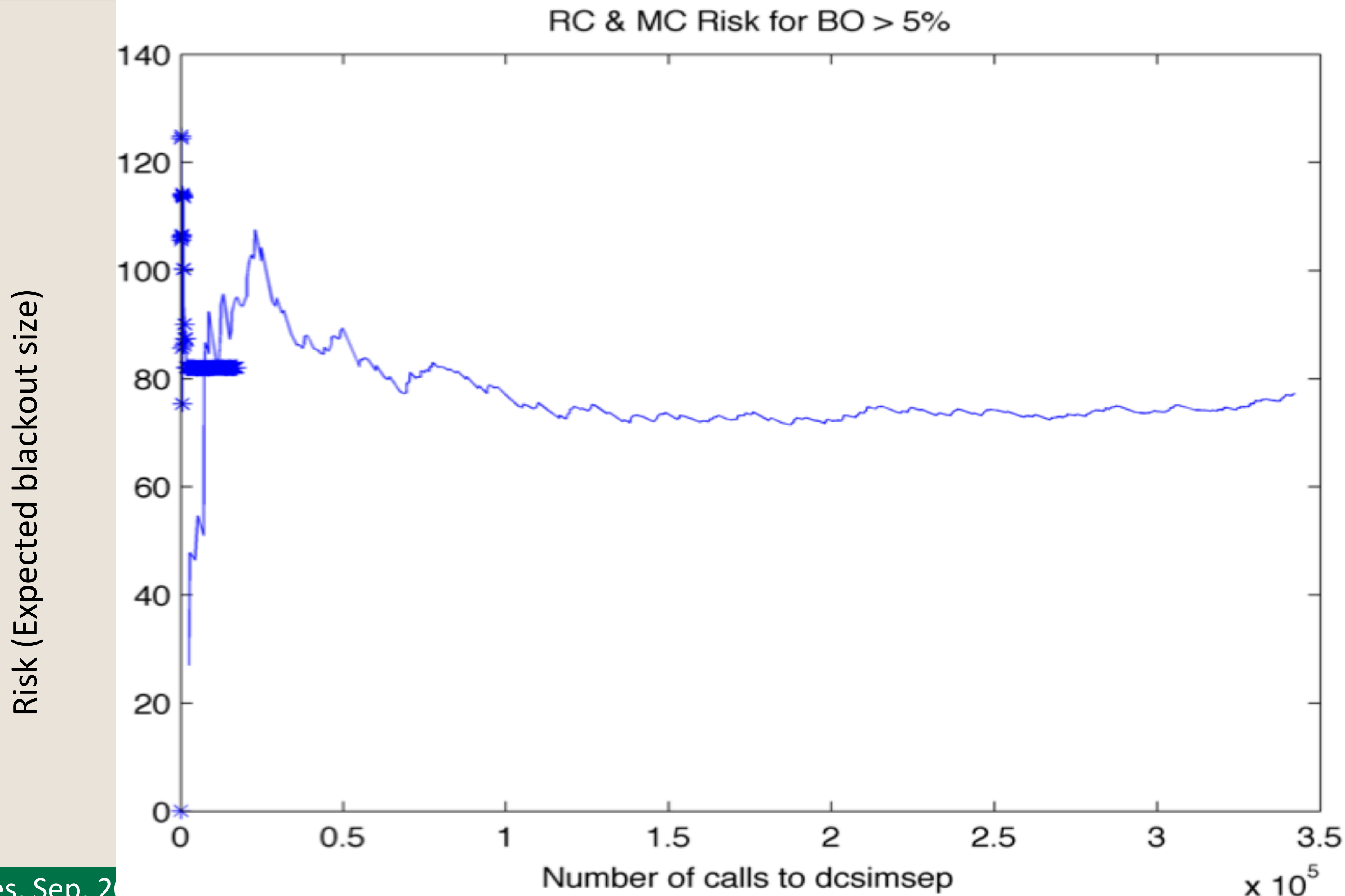


The collections show interesting patterns

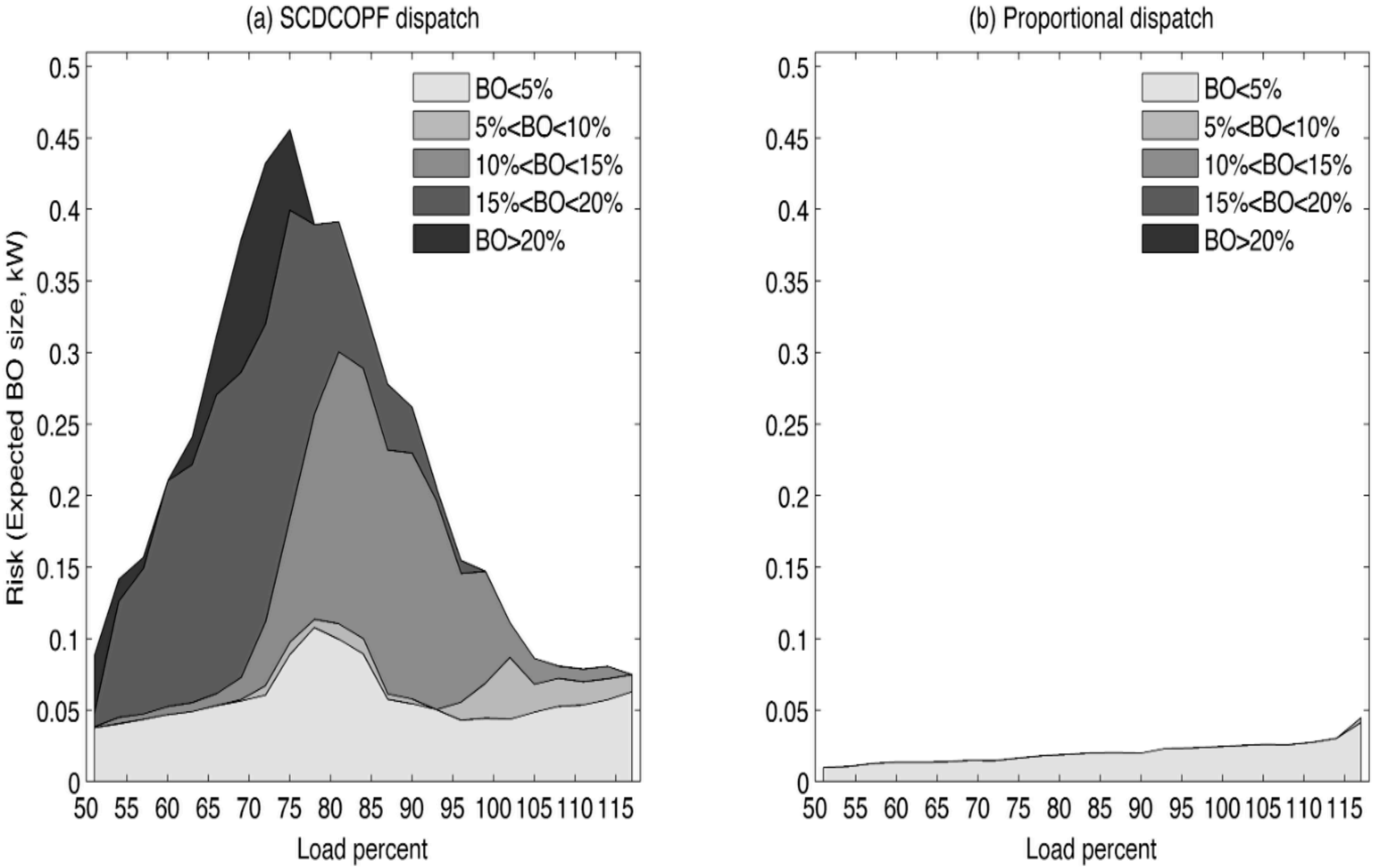


Hines, Sep. 2013

Using Random Chemistry to Estimate Risk



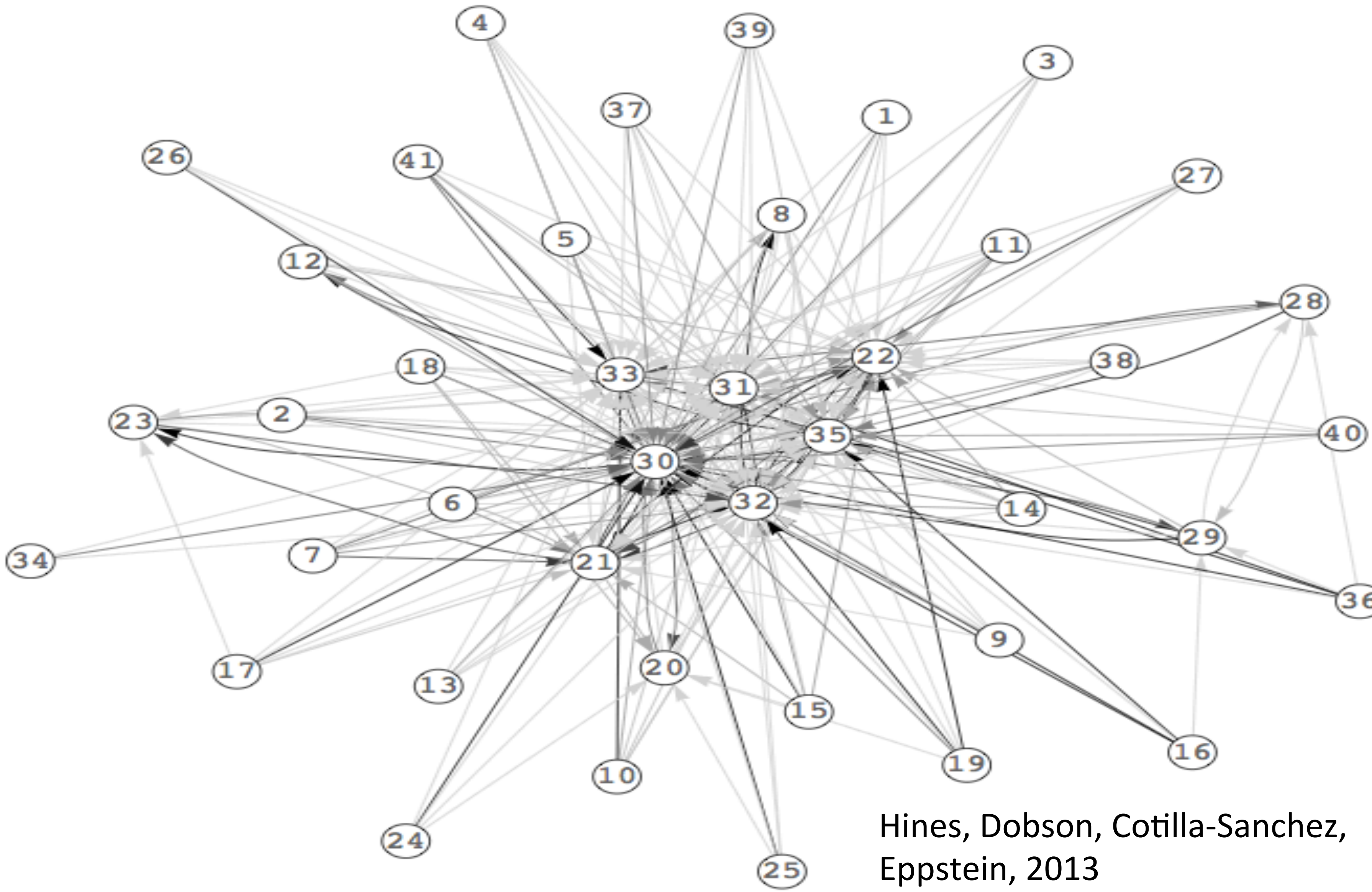
And now we can get useful insight



Are there ways to transform the data into useful structures?

- We now have millions of example cascades.
- Are there patterns in the sequences?
- Does the outage of 12 frequently follow 24?

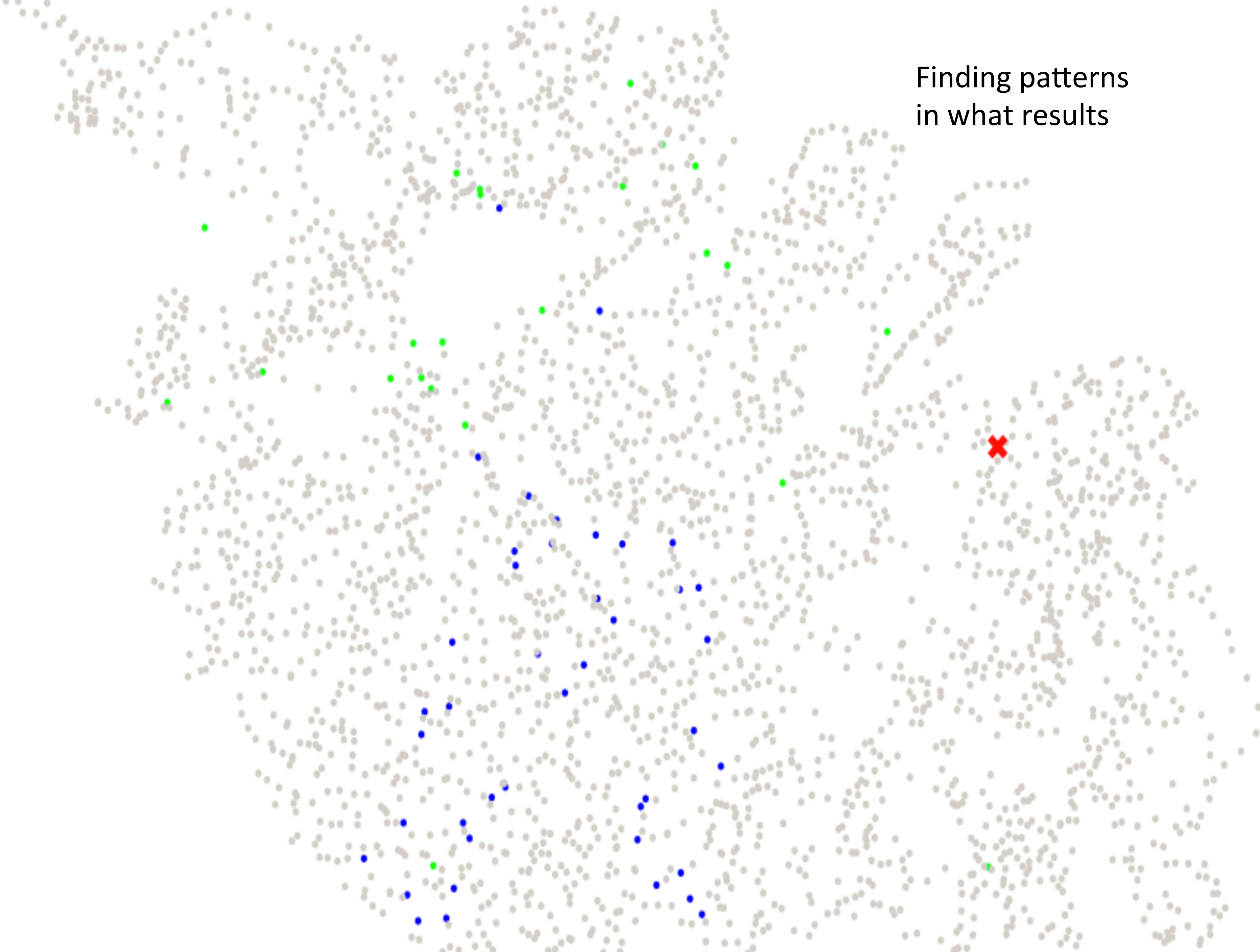
An "influence" graph



Hines, Dobson, Cotilla-Sanchez, Eppstein, 2013

An influence graph for the Polish Network

graph showing links with a weight of 1000 or greater



Finding patterns
in what results

Questions? Comments?

paul.hines@uvm.edu

@paulhinesuvm

uvm.edu/~phines

uvm.edu/complexsystems

Paul Hines, Ph.D.

University of Vermont

Rethinking Network Science and Modeling for Critical Infrastructure Protection, Analysis, and Development

McLean, VA. Sept. 10, 2013

NY City, Nov. 9, 1965