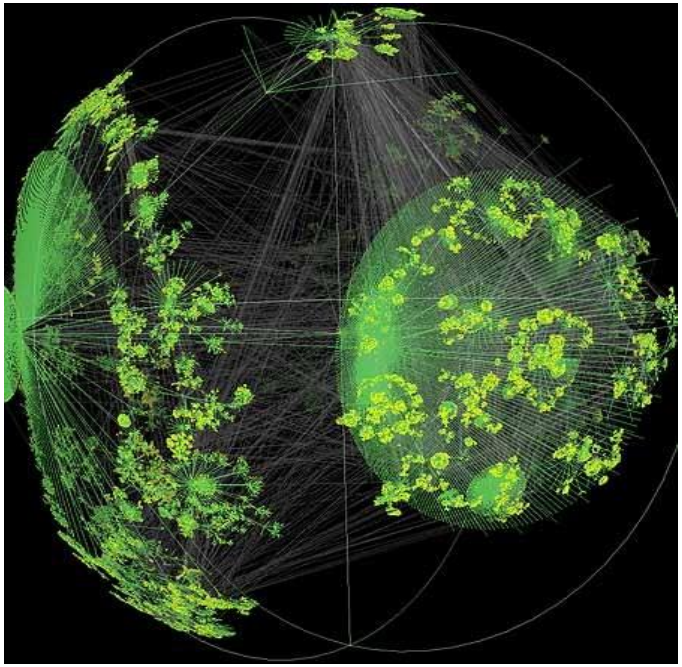
Strategic Analysis and Design of Robust and Resilient Interdependent Power and Communication Networks with a New Model of Interdependency



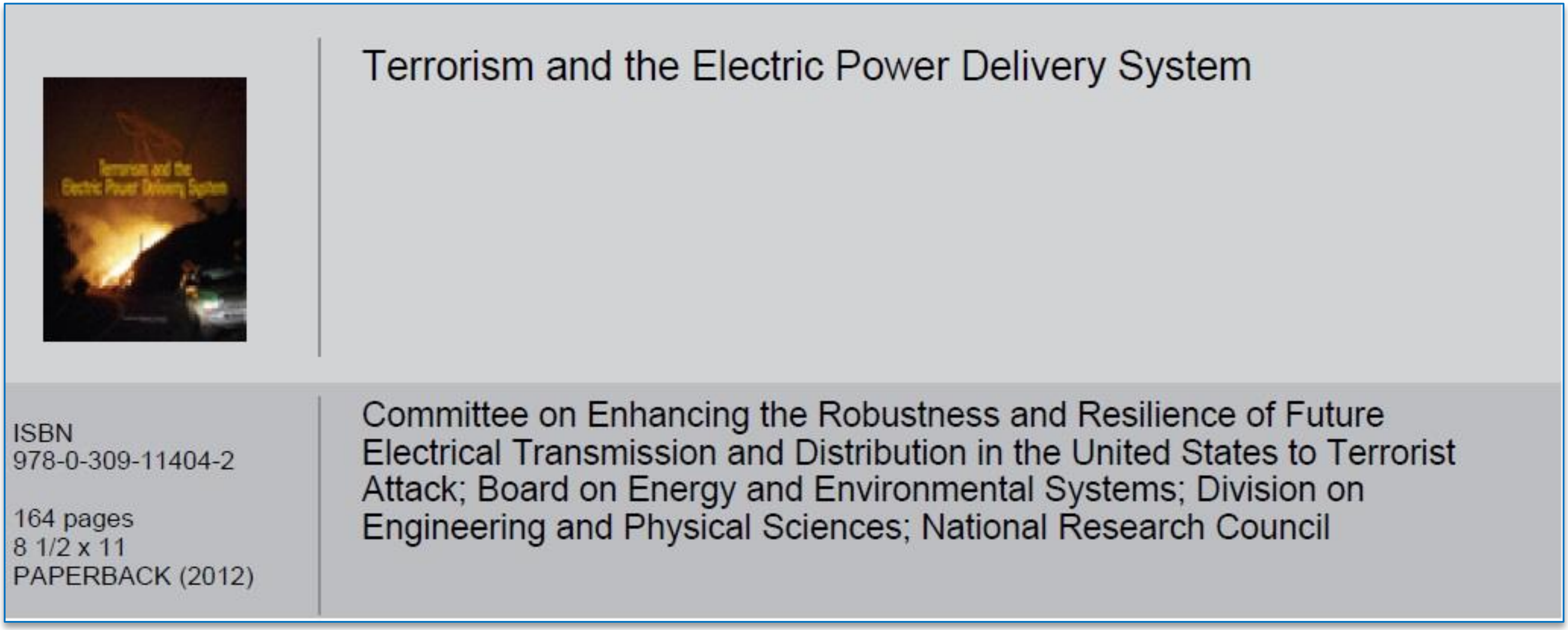
NEXT LAB

LABORATORY FOR THE SCIENCE OF NETWORKED EXISTENCE

Arun Sen
Computer Science Program
School of Computing, Informatics
and Decision Systems Engineering
Arizona State University

Background

The U.S. power delivery system is remarkably complex. It is a network of substations, transmission lines, distribution lines, and other components that people can see as they drive around the country; it also includes the less visible devices that sense and report on the state of the system, the automatic and human controls that operate the system, and the intricate web of computers and communication systems that tie everything together.



Terrorism and the Electric Power Delivery System

ISBN
978-0-309-11404-2

164 pages
8 1/2 x 11
PAPERBACK (2012)

Committee on Enhancing the Robustness and Resilience of Future Electrical Transmission and Distribution in the United States to Terrorist Attack; Board on Energy and Environmental Systems; Division on Engineering and Physical Sciences; National Research Council

Background

Since the Northeast Blackout of 1965, there has been an increasing integration of the power and telecommunications infrastructures. In particular, power systems have become increasingly dependent on the proper operation of supporting communication systems; failures in these supporting communications systems can result in system-wide blackouts. Blackouts that have been either directly caused by or aggravated by communication system failures have occurred in Europe as well as North America. Two clear examples of blackouts involving communication system elements have been experienced in the El Paso Electric (EPE) system and the Hydro-Québec system. In the EPE system, load was lost when a set of phase angle comparison relays improperly isolated a 345-kV transmission line. The improper operation of the relays was based on calculations using an incorrect communications latency value [2]. In the Hydro-Québec system, load was lost when a special protection system (SPS) experienced a single point failure in the supporting communications system [3]. In both cases, the loss of load could have been minimized if the interactions between the power and telecommunications infrastructures had been analyzed systematically. One of the reasons that this analysis was not performed is that there are limited tools for the systematic analysis of infrastructure interactions.

IEEE TRANSACTIONS ON POWER SYSTEMS, VOL. 21, NO. 3, AUGUST 2006 1123
Assessment of Interactions Between Power and Telecommunications Infrastructures
Kevin Schneider, *Member, IEEE*, Chen-Ching Liu, *Fellow, IEEE*, and Jean-Philippe Paul

NSF RIPS
(Resilient Interdependent Infrastructure Processes and Systems)

Background

NSF RIPS CFP

- The goals of the Resilient Interdependent Infrastructure Processes and Systems (RIPS) solicitation are
  - (1) to foster an interdisciplinary research community that discovers new knowledge for the design and operation of infrastructures as processes and services
  - (2) to enhance the understanding and design of interdependent critical infrastructure systems (ICIs) and processes that provide essential goods and services disruptions and failures from any cause, natural, technological, or malicious, and
  - (3) to create the knowledge for innovation in ICIs to advance society with new goods and services.

NSF RIPS CFP

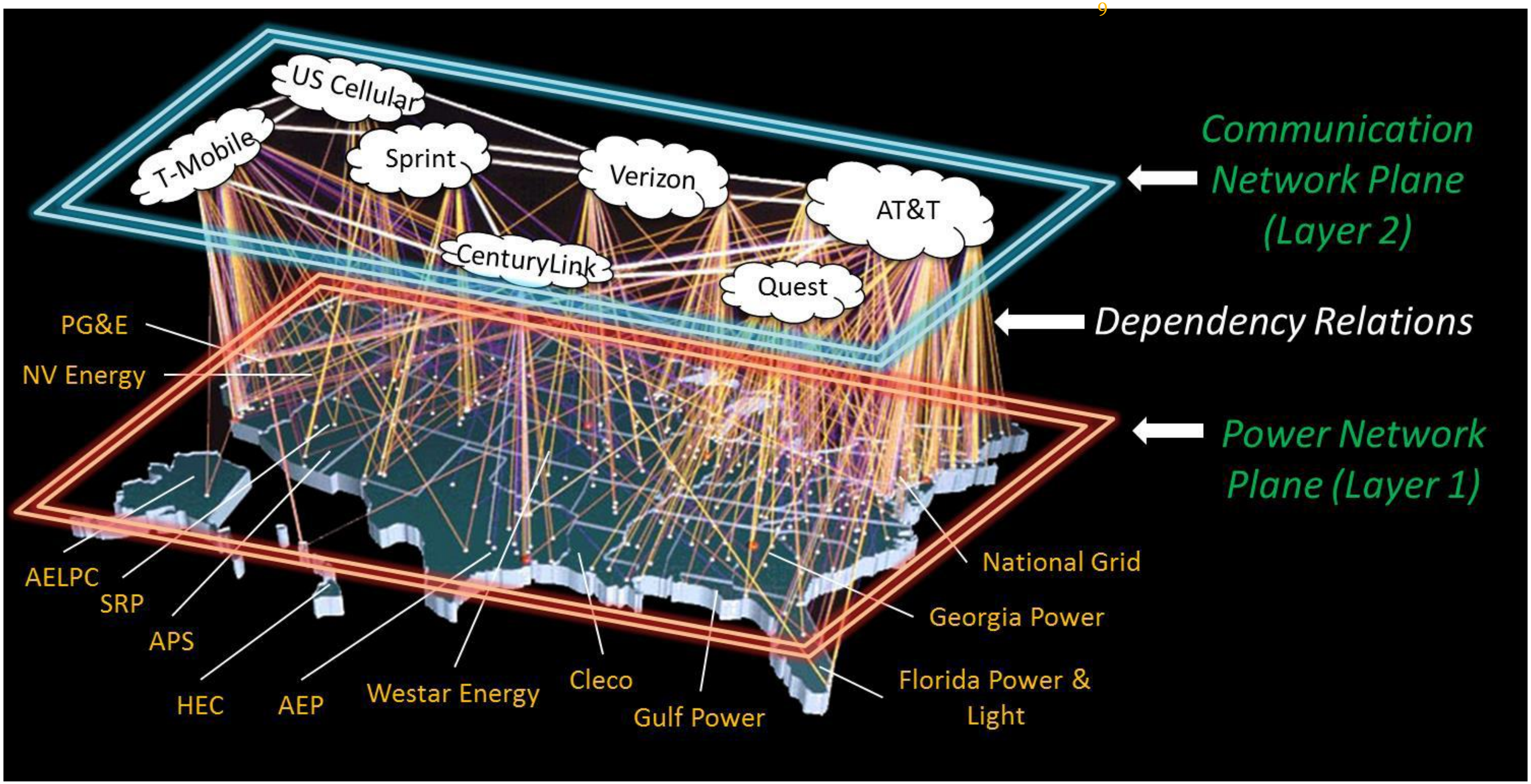
- The objectives of this solicitation are:
  - Create theoretical frameworks and multidisciplinary computational models of interdependent infrastructure systems, processes and services, capable of analytical prediction of complex behaviors, in response to system and policy changes
  - Synthesize new approaches to increase resilience, interoperations, performance, and readiness in ICIs
  - Understand organizational, social, psychological, legal, political and economic obstacles to improving ICI's, and identifying strategies for overcoming those obstacles

NSF RIPS CFP

- Successful proposals are expected to study multiple infrastructures focusing on them as interdependent systems that deliver services, enabling a new interdisciplinary paradigm in infrastructure research
- Proposals that do not broadly integrate across the cyber-physical, engineering and social, behavioral and economic (SBE) sciences may be returned without review
- Projects supported under this solicitation may undertake the collection of new data or use existing curated data depending on the category of award, and must recognize that a primary objective is integrative predictive modeling that can use the data to validate the models and which can be integrated into decision making.

Vulnerability Assessment of Multi-Layer Interdependent Networks

Focus Areas



Interdependent critical infrastructure systems comprising of Power and Communication Networks

More than 90 percent of the U.S. power grid is privately owned and regulated by the states, making it challenging for the federal government to address potential vulnerabilities to its operation, and perhaps especially its vulnerability to terrorist attack.

- One of the goals of the RIPS program is to increase resilience in ICIs
  - How do you measure resiliency of ICIs?
    - Is there a metric to measure resiliency?
      - If there is no such metric, maybe a metric should be defined to measure resiliency
      - Without a metric it may be impossible to make a statement about how secure or vulnerable our integrated power-communication infrastructure is
      - With such a metric it maybe possible to make a statement that resiliency of our current ICI's is at level X
      - If level X resiliency is inadequate, how to augment the ICI to reach level Y with least cost?

- If indeed there is no such known technique to measure resilience/vulnerability of ICIs, maybe efforts should be made to develop such techniques
- Similar examples:
  - There is a way to measure strength of a hurricane – Sandy was a category 4 hurricane
  - Military readiness level is also categorized
  - The notion of “reliability” of a system has some similarity to the notion of resilience/vulnerability
    - Reliability Theory is a very well established discipline
  - To the best of our knowledge there is no such theory of vulnerability or resilience
  - Just as it is possible to measure the strength of a hurricane or preparedness of a military, there should be a way to measure vulnerability and/or resilience of ICIs

- Insurance officials assess risk of damage to infrastructures and determine the insurance premium
  - Risk Analysis is also an established discipline
  - Maybe such techniques will be useful in determining vulnerability of ICIs

- Security/vulnerability of ICIs need to be addressed w.r.t. the type of eventuality, e.g., natural disasters, cyber attacks, physical attacks, etc.

- Severity of an attack should also be categorized (measurable)

- In the previous slides we made some observations and raised some questions regarding vulnerability/resilience of ICIs

- What type of analysis will be necessary to answer those questions?

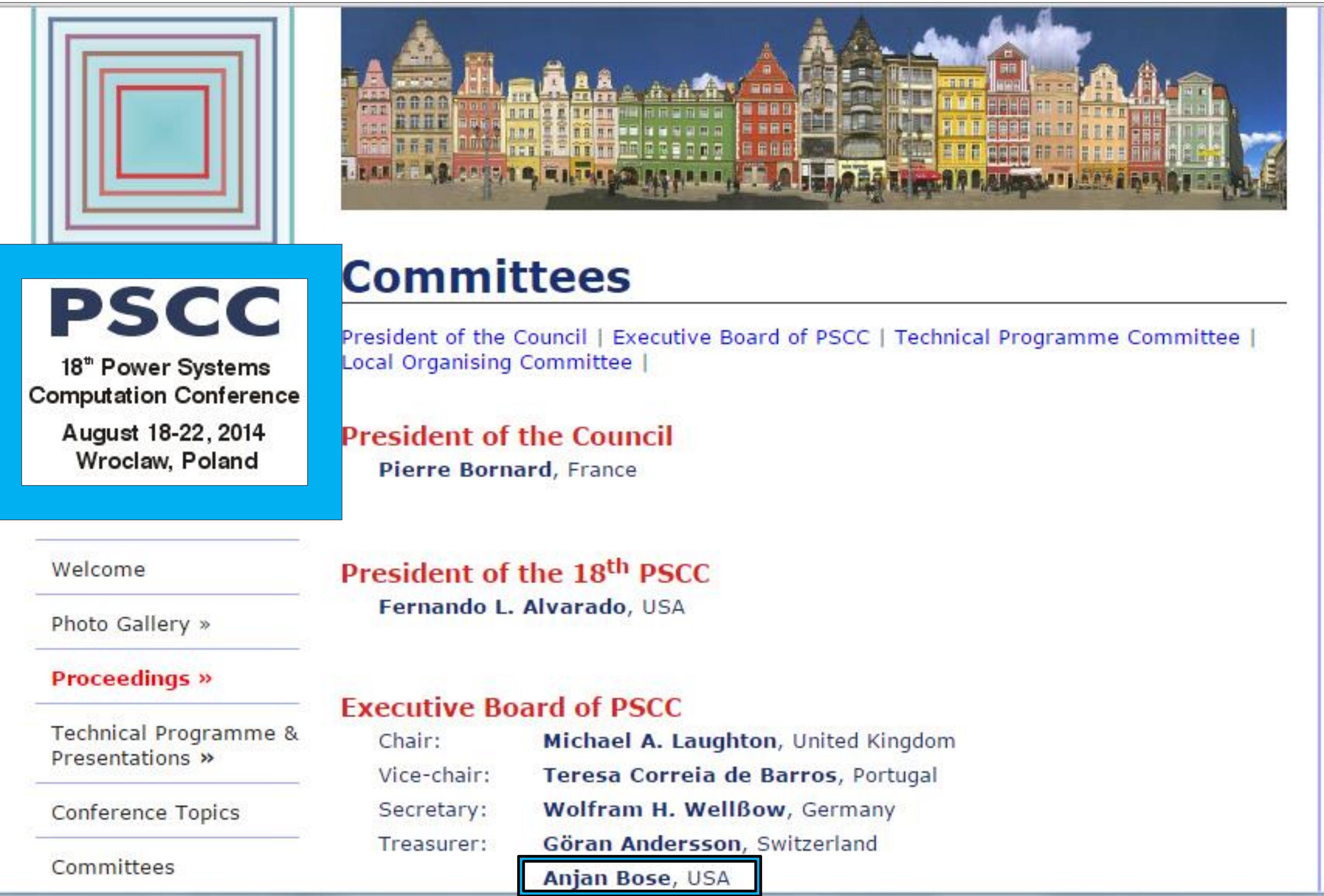
- Are those questions worthy enough to spend time and effort to find answers?

- In our earlier conversations we discussed “microscopic” and “macroscopic” analysis
- What is our notion of microscopic and macroscopic analysis?
- What type of questions can be answered through microscopic analysis?
- What type of questions can be answered through macroscopic analysis?
- Is one type of analysis adequate to answer the questions raised earlier?

- The goal of the RIPS program is to “create theoretical frameworks and multidisciplinary computational models of interdependent infrastructure systems”

- What are the current models of interdependent infrastructure systems?
  - With particular reference to interdependence between power and communication networks

- In the past few years quite a few models of interdependent infrastructure systems have been proposed without any effort of validating any one of them.



PSCC

18th Power Systems Computation Conference

August 18-22, 2014
Wroclaw, Poland

Committees

President of the Council | Executive Board of PSCC | Technical Programme Committee | Local Organising Committee |

President of the Council

Pierre Bornard, France

President of the 18th PSCC

Fernando L. Alvarado, USA

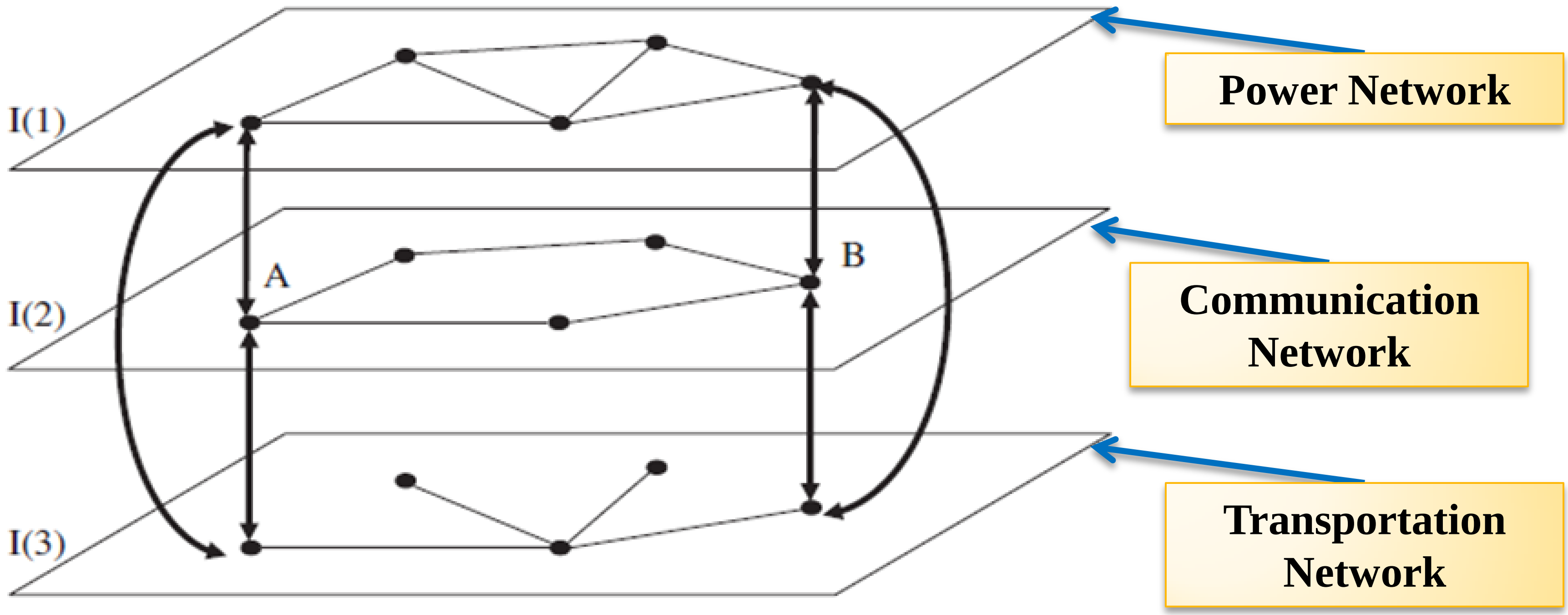
Executive Board of PSCC

Chair:	**Michael A. Laughton**, United Kingdom
Vice-chair:	**Teresa Correia de Barros**, Portugal
Secretary:	**Wolfram H. Wellßow**, Germany
Treasurer:	**Göran Andersson**, Switzerland
	Anjan Bose, USA

Modeling Interdependent Infrastructure Networks

Limitations of Existing Models & Proposed New Model

Multilayered Complex Network



Power Network

Communication Network

Transportation Network

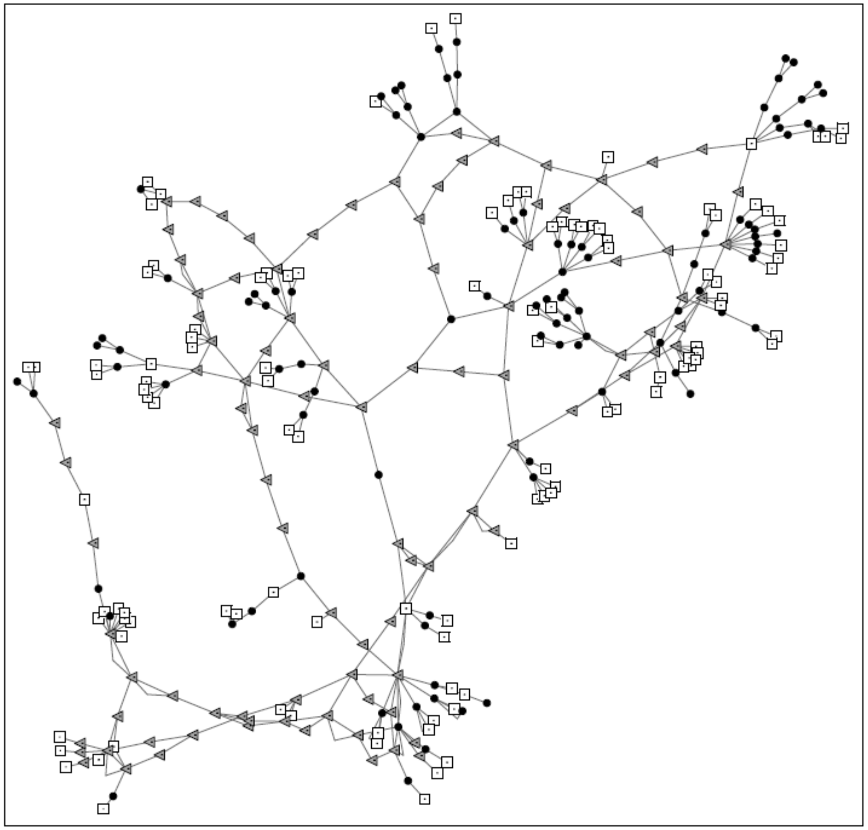
Multiplicity of Models

- Many models have been proposed in the last few years
- For example:
  - Rosato Model (2008)
  - Buldyrev Model (2010)
  - Peeta Model (2011)
  - Castet Model (2012)
  - Liu Model (2012)
  - Modiano Model (2013)

Multiplicity of Models

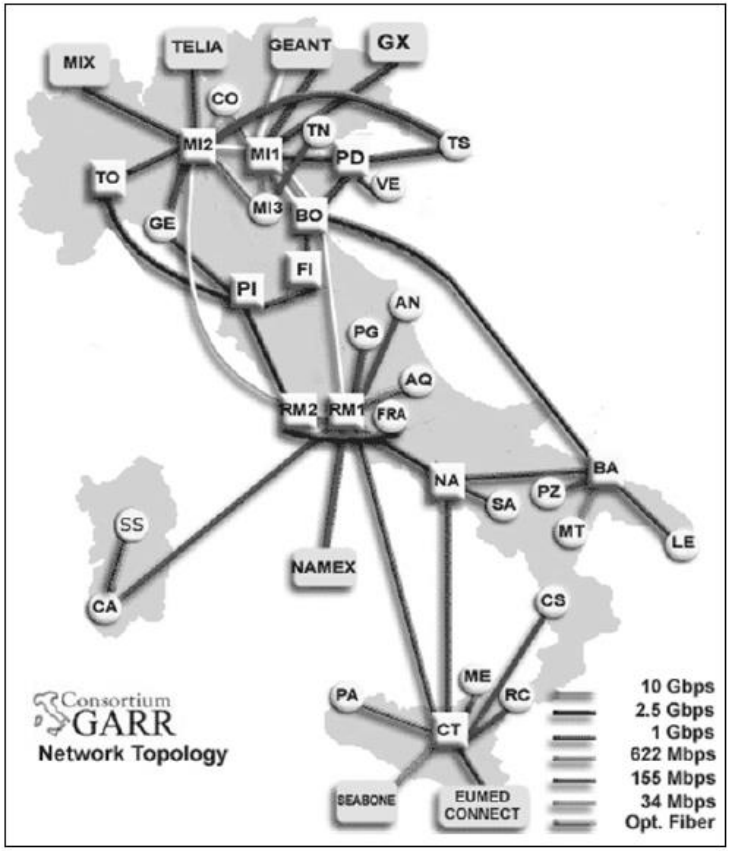
The Rosato Model (2008)

Figure 1 The graph corresponding to the Italian high-voltage (380 kV) transmission grid resulting from the available data.



Notes: Source *S* nodes are square, Load *L* nodes triangles and Junction *J* nodes are black circles

Figure 4 The high-bandwidth backbone of the internet network dedicated to linking Italian universities and research institutions (GARR)



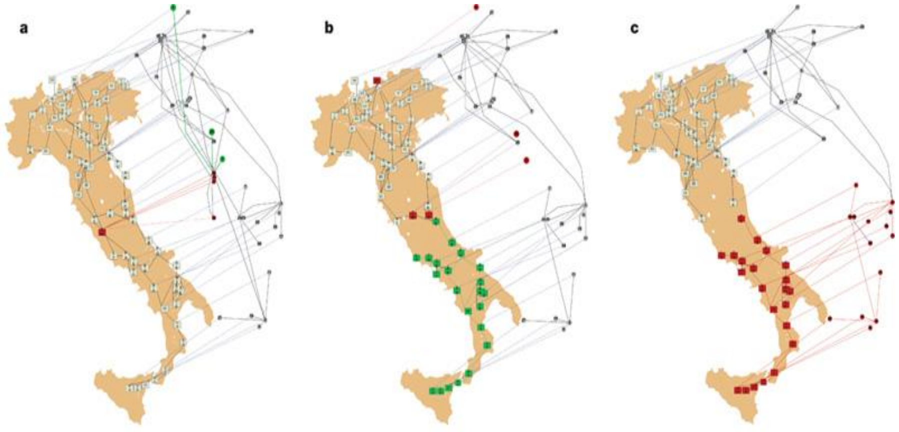
Multiplicity of Models

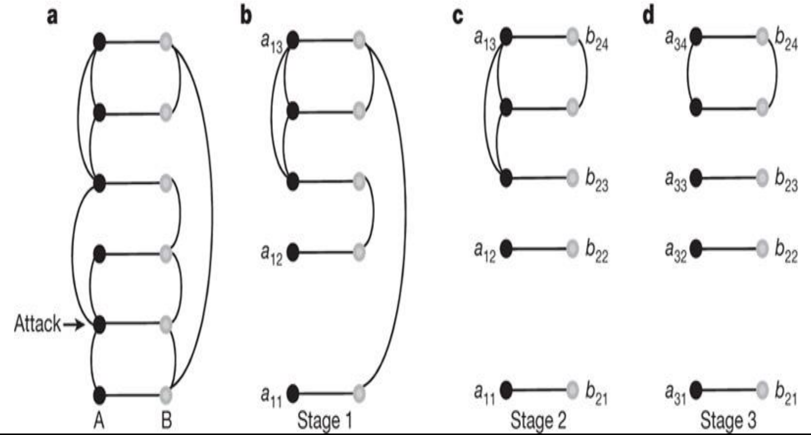
The Rosato Model (2008)

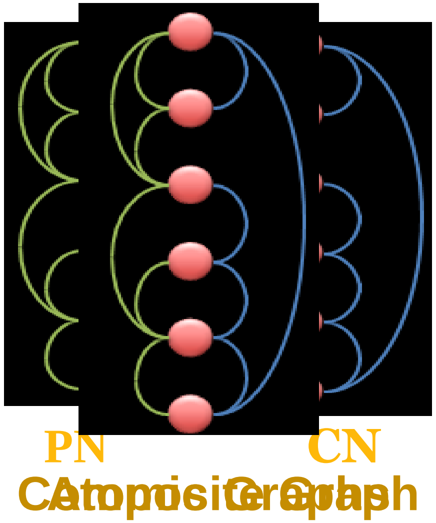
- Realistic modeling of Power Network (PN) and Communication Network (CN)
- Effect of perturbation of PN on CN is analyzed based on a coupling parameter
- The impact of CN on PN is not analyzed
- The coupling parameter is not validated and is assumed

Multiplicity of Models

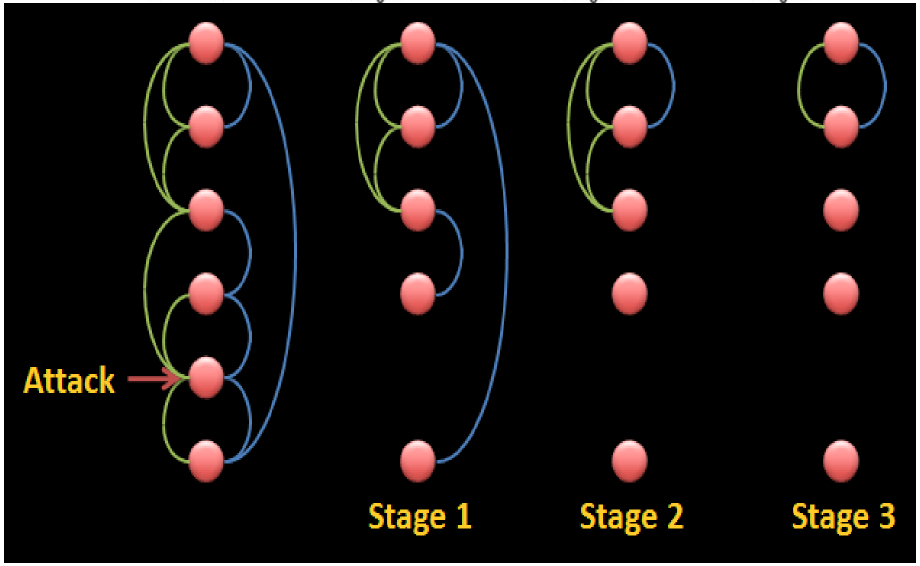
The Buldyrev Model (2010)







Blue edge for CN
Green edge for PN



A component in a composite graph is connected if any two nodes have at least one blue path and one green path connecting them.

Multiplicity of Models

The Buldyrev Model (2010)

- Fault propagation with both intra link connection and inter link interdependencies in consideration
- Network robustness --- maximum number of node removal from one network to get at least one giant connected cluster (percolation threshold)
- Nodes in PN not designated as generator, substations or load and in CN not designated as routers or control centers
- Actual working of SCADA system in CN needs to be considered in modeling interdependency

Multiplicity of Models

The Buldyrev Model (2010)

The transients and readjustments of the system can be local in effect or can involve components far away, so that a component disconnection or failure can effectively increase the loading of many other components throughout the network. In particular, the propagation of failures is not limited to adjacent network components.

- to appear in Probability in the Engineering and Informational Sciences, 2005
- submitted February 2004, accepted April 2004
- A LOADING-DEPENDENT MODEL OF
- PROBABILISTIC CASCADING FAILURE
- Ian Dobson
- Electrical & Computer Engineering Department
- University of Wisconsin-Madison
- 1415 Engineering Drive
- Madison WI 53706 USA
- phone 608 262 2661
- fax 608 262 1267
- Email: dobson@engr.wisc.edu

Multiplicity of Models

The Peeta Model (2011)

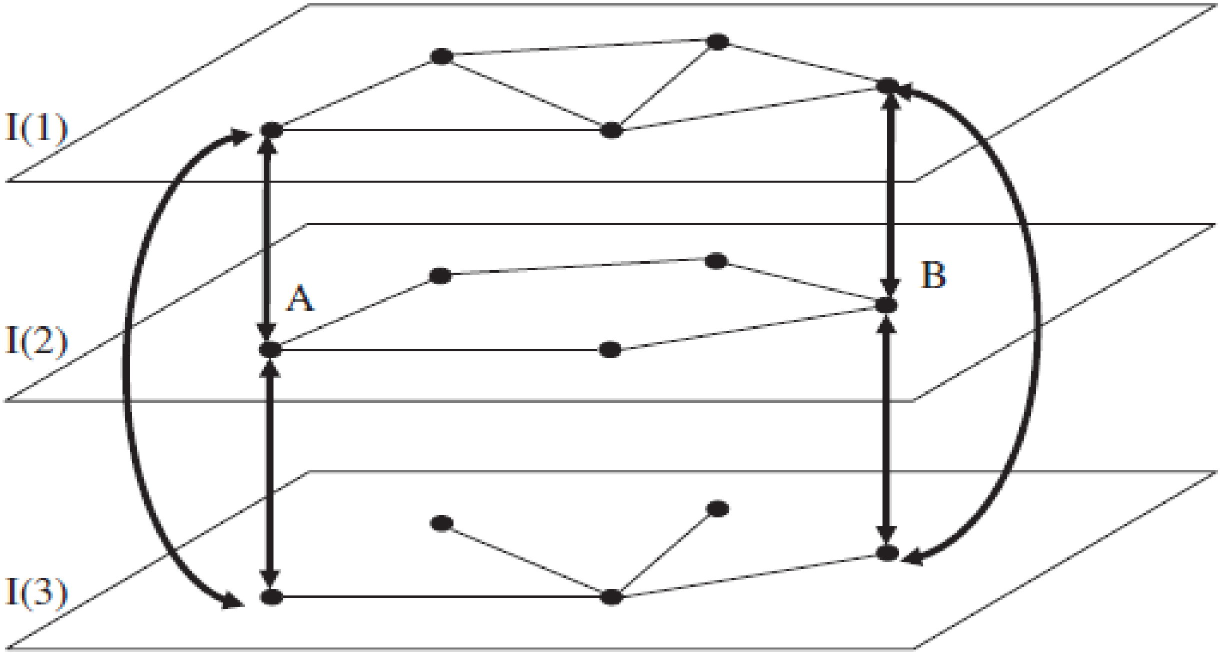
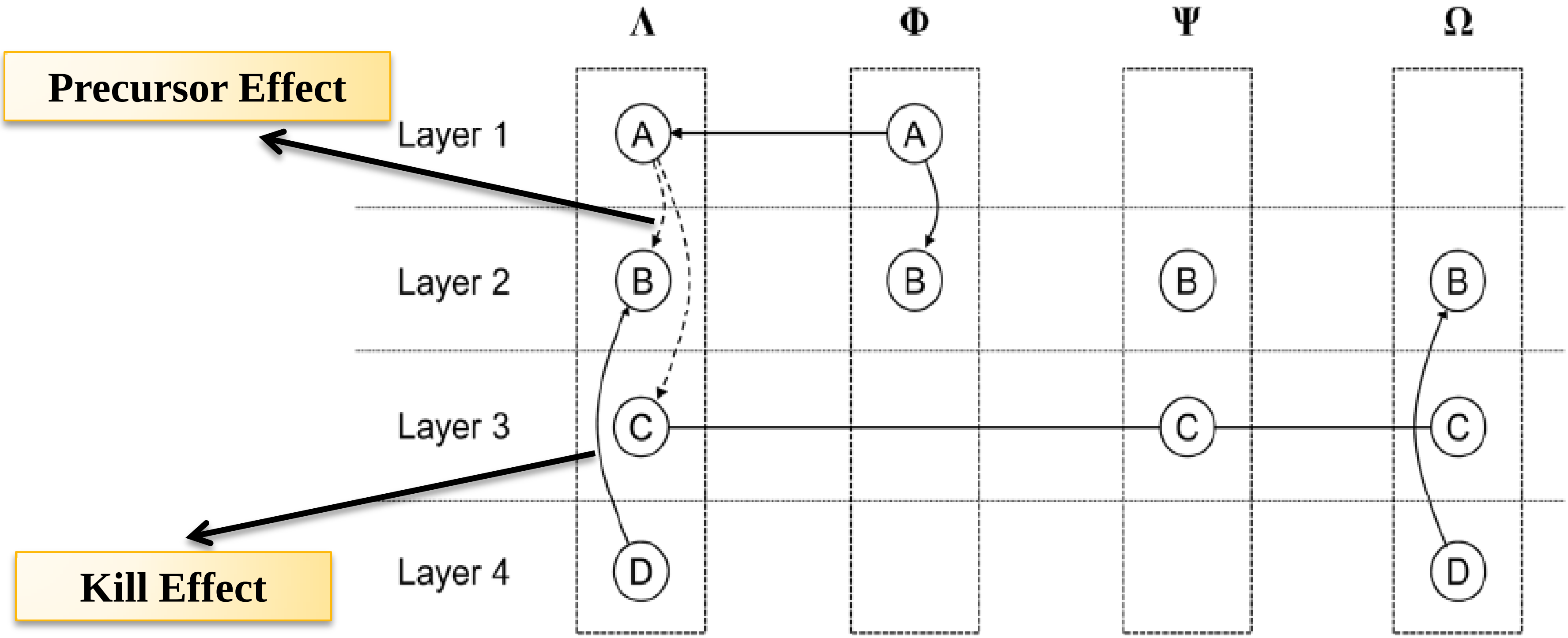


Fig. 1. Multilayer infrastructure network (MIN) framework.

Multiplicity of Models

The Castet Model (2012)



Precursor Effect

Kill Effect

Figure 3. General representation of an Interdependent Multi-Layer Network.

Multiplicity of Models

The Castet Model (2012)

- Interdependency in space based networks with shared subsystems

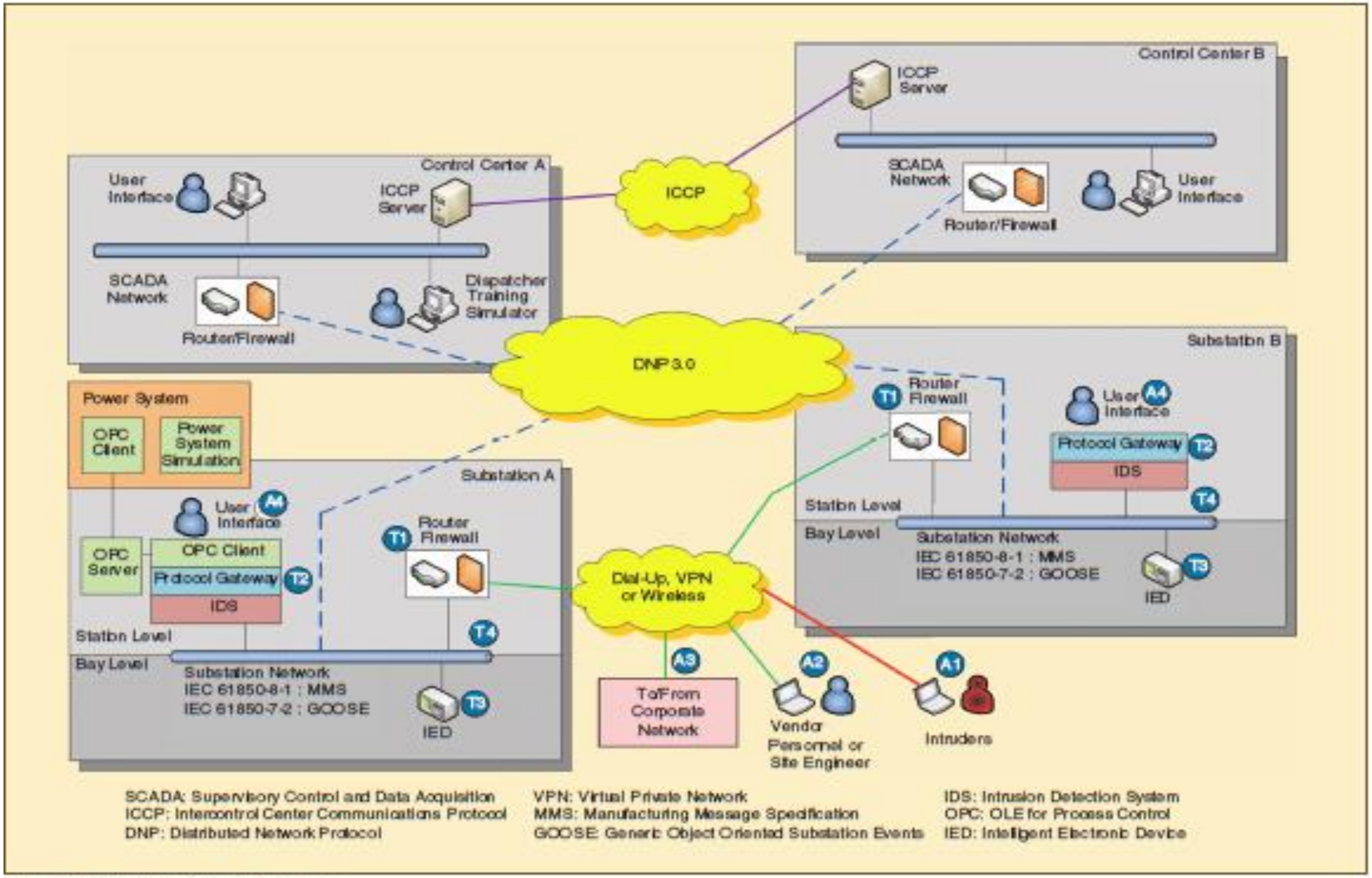
- Two different type of interdependency among different subsystems --- kill effect and precursor effect

- A failure propagation algorithm is developed

- The cases considered in experiments though realistic are not validated

Multiplicity of Models

The Liu Model (2012)

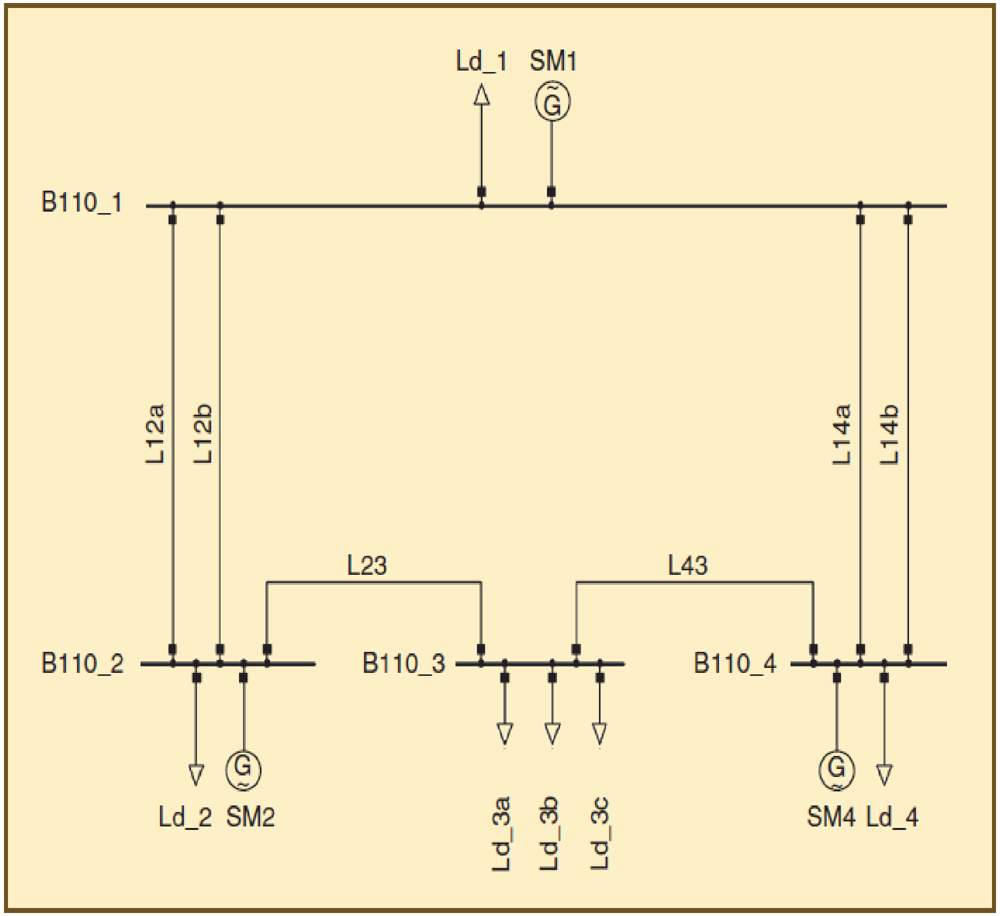


SCADA: Supervisory Control and Data Acquisition
ICCP: Intercontrol Center Communications Protocol
DNP: Distributed Network Protocol
VPN: Virtual Private Network
MMS: Manufacturing Message Specification
GOOSE: Generic Object Oriented Substation Events
IDS: Intrusion Detection System
OPC: OLE for Process Control
IED: Intelligent Electronic Device

figure 2. Cybersecurity test bed at UCD.

Multiplicity of Models

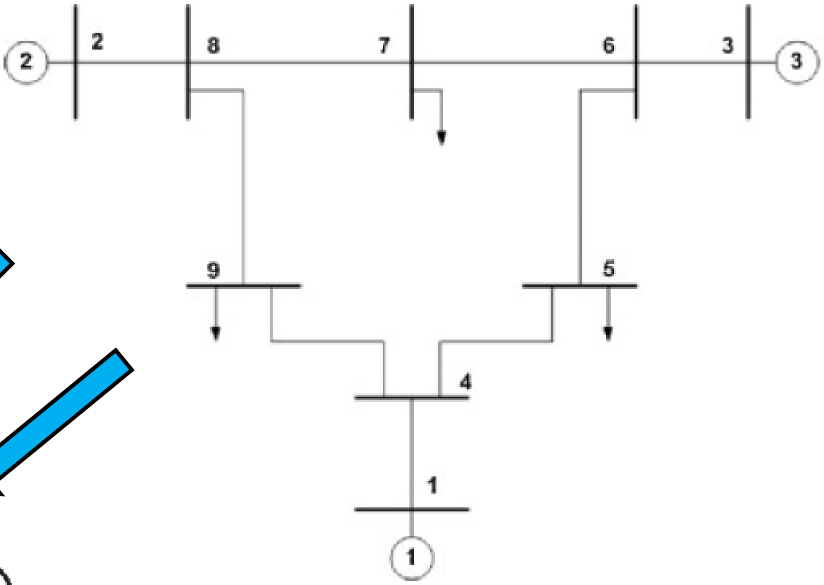
The Liu Model (2012)

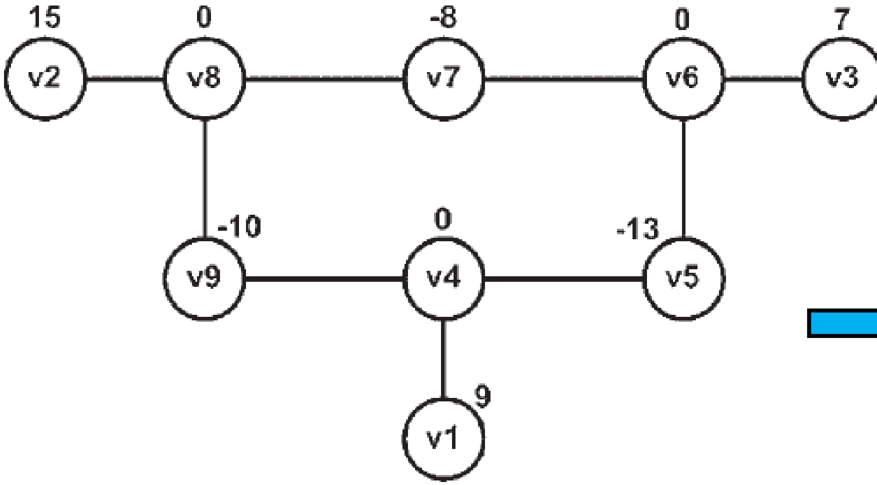


- Effect of cyber intrusions in SCADA and EMS system on PN is analyzed through realistic test beds
- The experiments are confined to small domain
- Large cascades of failure owing to this effect is not analyzed

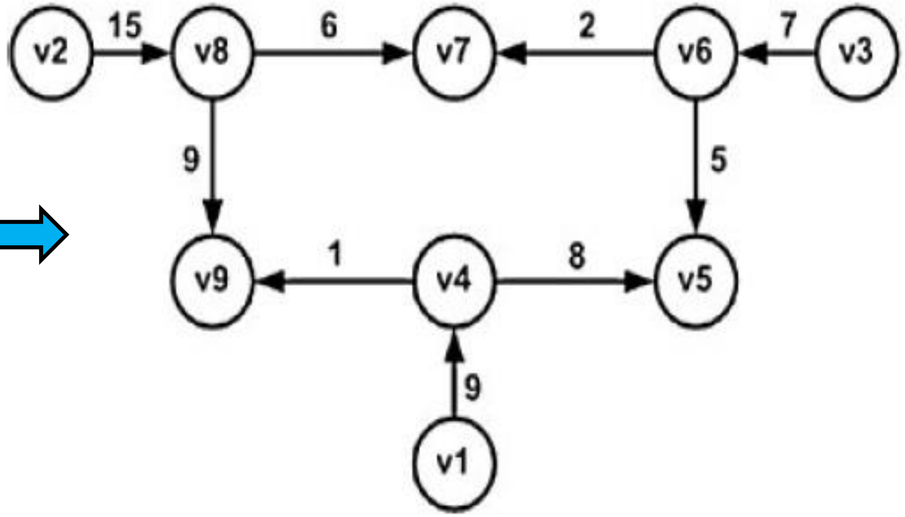
Multiplicity of Models

WSCC 9 Bus System





Node weighted graph model with generator and load weights



Edge weighted graph model with power flow nn the transmission links

Multiplicity of Models

The Modiano Model (2013)

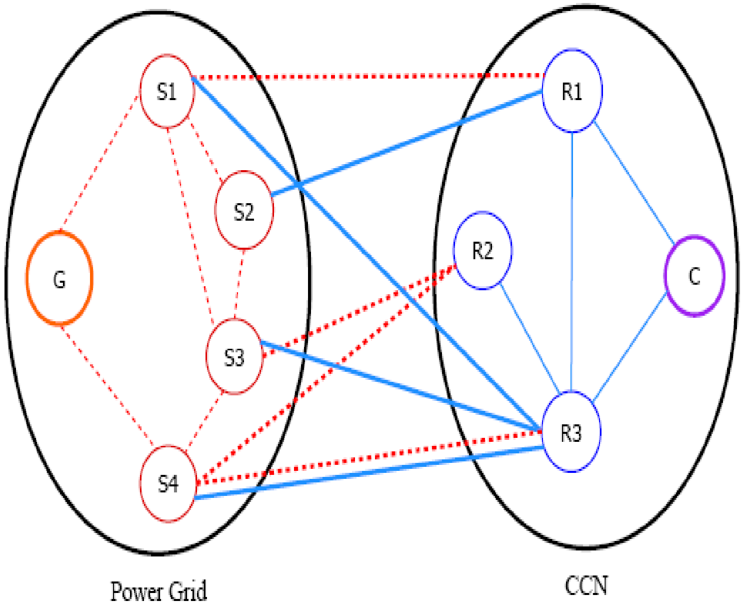
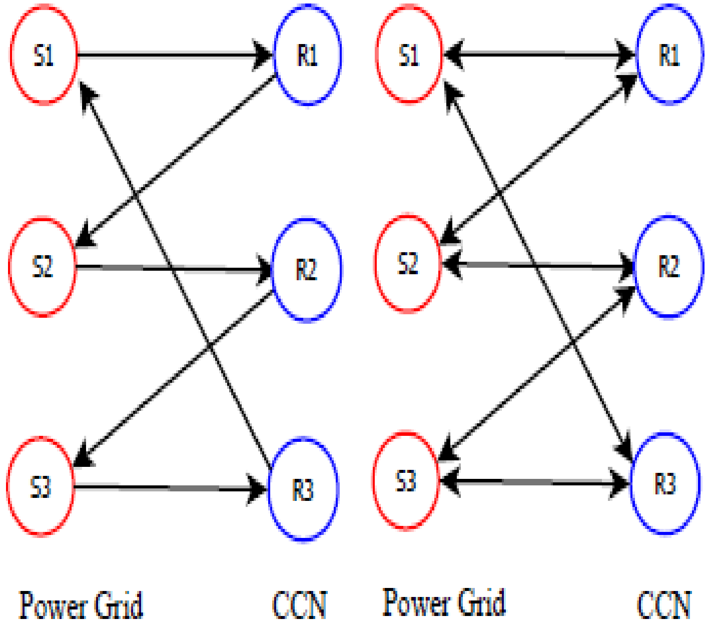


Fig. 1. Cyber-Physical Interdependency Model - dotted lines represent power lines and solid lines represent communication lines

In this model, a substation operates if it has a path to a generator, i.e. receives power and it is also connected to a router, i.e. sends data and receives control signals. Similarly, we say that a router operates if it has a path to a control center, i.e. sends data and receives control signals and it is also connected to a substation, i.e. receives power.

Multiplicity of Models

The Modiano Model (2013)



a) Unidirectional Interdependency (b) Bidirectional Interdependency

Fig. 3. Graph structure under different interdependency models

Both networks have star topologies.

All of the substations in the power grid are directly connected to the generator;

No substation's failure can disconnect the other substations from the generator.

All of the routers in the CCN are directly connected to the control center, and

No router's failure can disconnect the other routers from the control center.

The failure of all nodes in both networks is known as Total Failure.

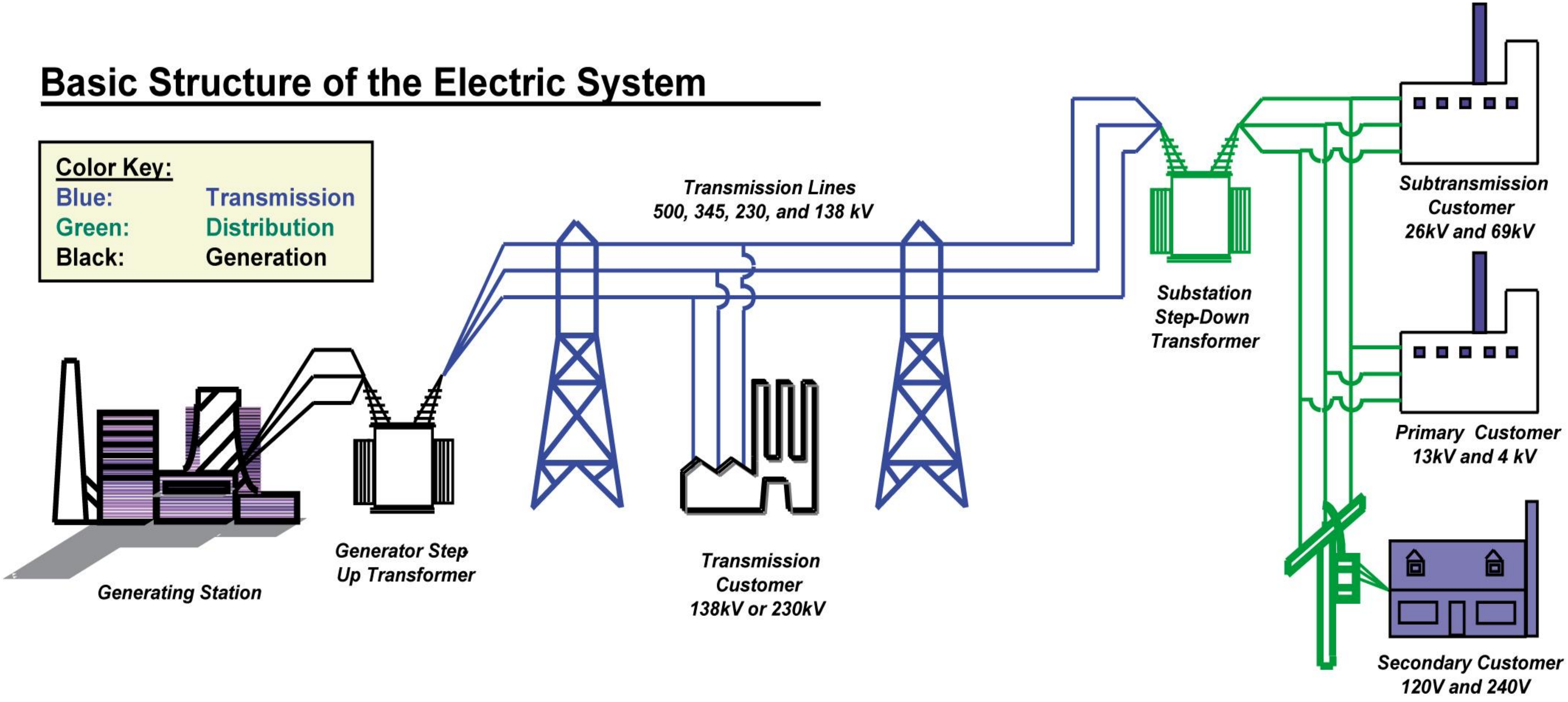
Q: What is the minimum number of nodes whose removals will lead to total failure?

Limitations of Current Models

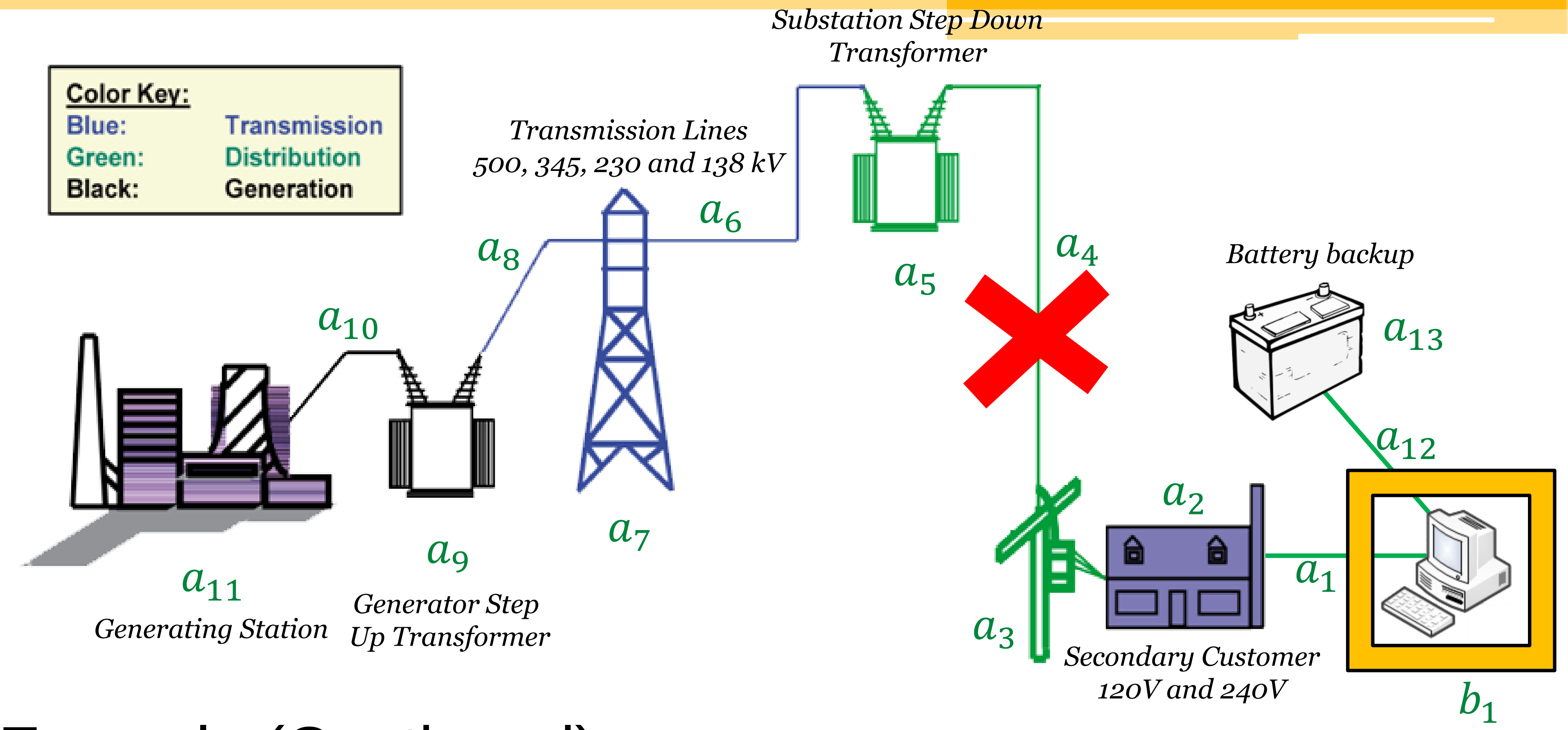
- Dependencies that exist between the entities of the Power and Communication networks are often complex, involving a combination of conjunctive and disjunctive terms representing the entities of these two types of networks.

- Most of the proposed interdependency models are unequipped to capture such complex interdependencies.

Example



Basic Structure of the Electric System



Example (Continued)

$$\checkmark\, b_1 \leftarrow \cancel{a_1 a_2 a_3 \xcancel{a_4} a_5 a_6 a_7 a_8 a_9 a_{10} a_{11}} + a_{12} a_{13}$$

An example of limitation of the current models

- Power Network Entity PNE_a (say, a generator, substation, transmission line, load) is “alive” if communication network entities
  - CNE_b and CNE_c and CNE_d are alive, OR
  - CNE_e and CNE_f are alive, OR
  - CNE_g is alive

- Examples of communication network entities may include routers, cell towers, fiber optic lines, optical signal amplifiers.

An example of limitation of the current models (continued)

- We introduce a new model to capture such complex dependencies using Boolean logic.
- We express the dependency relation in the example in the previous slide in the following way:

$$\boxed{PNE_a \leftarrow CNE_b CNE_c CNE_d + CNE_e CNE_f + CNE_g}$$

- This dependency relation is a necessary but not sufficient condition for PNE$_a$ to be **“alive”**.

Cascading Failures in Multi-layered Networks

- Failures in a multi-layered network can cascade from layer to layer.

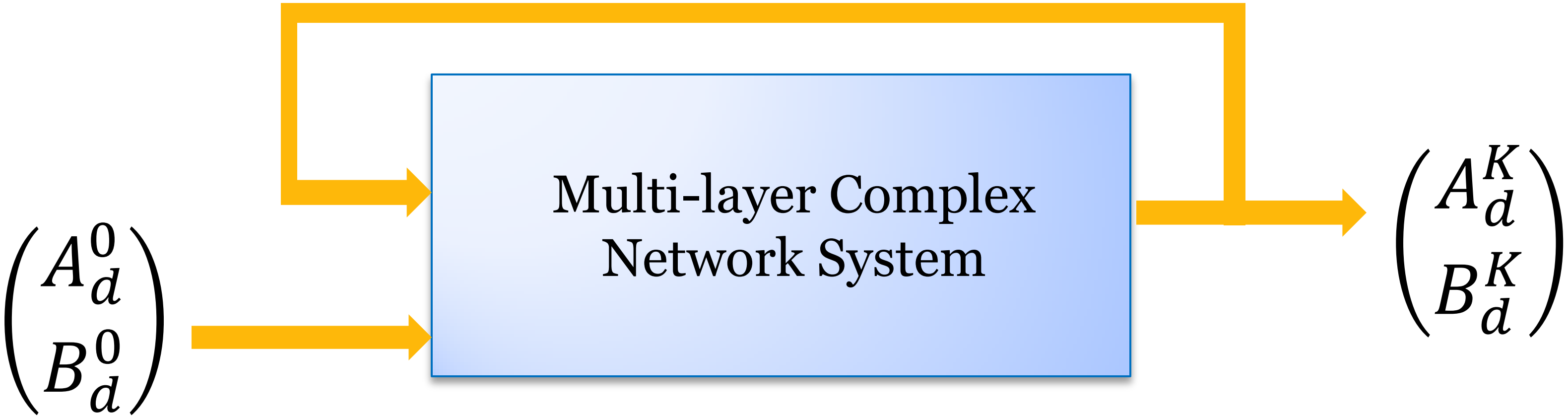
- CNE’s such as routers can not operate without power and PNE’s such as Supervisory Control and Data Acquisition Systems (SCADA) can not operate without control signals received through communication network.

Cascading Failures in Multi-layered Networks

- Failures propagate in time steps.
- We denote PNE’s as type A entities and CNE’s as type B entities.
- Let Boolean variables ‘a’ and ‘b’ to indicate the states of the entities.
- Cascading failures reach a steady state after K time steps.

$$\begin{tikzcd}
A_d^0 \arrow[dr] & A_d^1 \arrow[dr] & A_d^2 \arrow[dr] & {} & \cdots & {} \arrow[dr] & A_d^{K-1} \arrow[dr] & A_d^K \\
B_d^0 \arrow[ur] & B_d^1 \arrow[ur] & B_d^2 \arrow[ur] & {} & & {} \arrow[ur] & B_d^{K-1} \arrow[ur] & B_d^K
\end{tikzcd}$$

Multilayer Complex Network System


$\begin{pmatrix} A_d^0 \\ B_d^0 \end{pmatrix}$
Multi-layer Complex Network System
$\begin{pmatrix} A_d^K \\ B_d^K \end{pmatrix}$

Multi-layer Interdependent Networks as Closed Loop Feedback Control System

Steady State in a Multilayered Complex Network System corresponds to a "***fixed point***" in the system:

$$f\left(A_d^K \cup B_d^K\right) = A_d^K \cup B_d^K$$

An Example

Power Network

$a_1 \leftarrow b_1 + \mathrm{b}_2$

$a_2 \leftarrow b_1 b_3 + b_2$

$a_3 \leftarrow b_3 b_1 b_2$

$a_4 \leftarrow b_1 + b_2 + b_3$

Communication Network

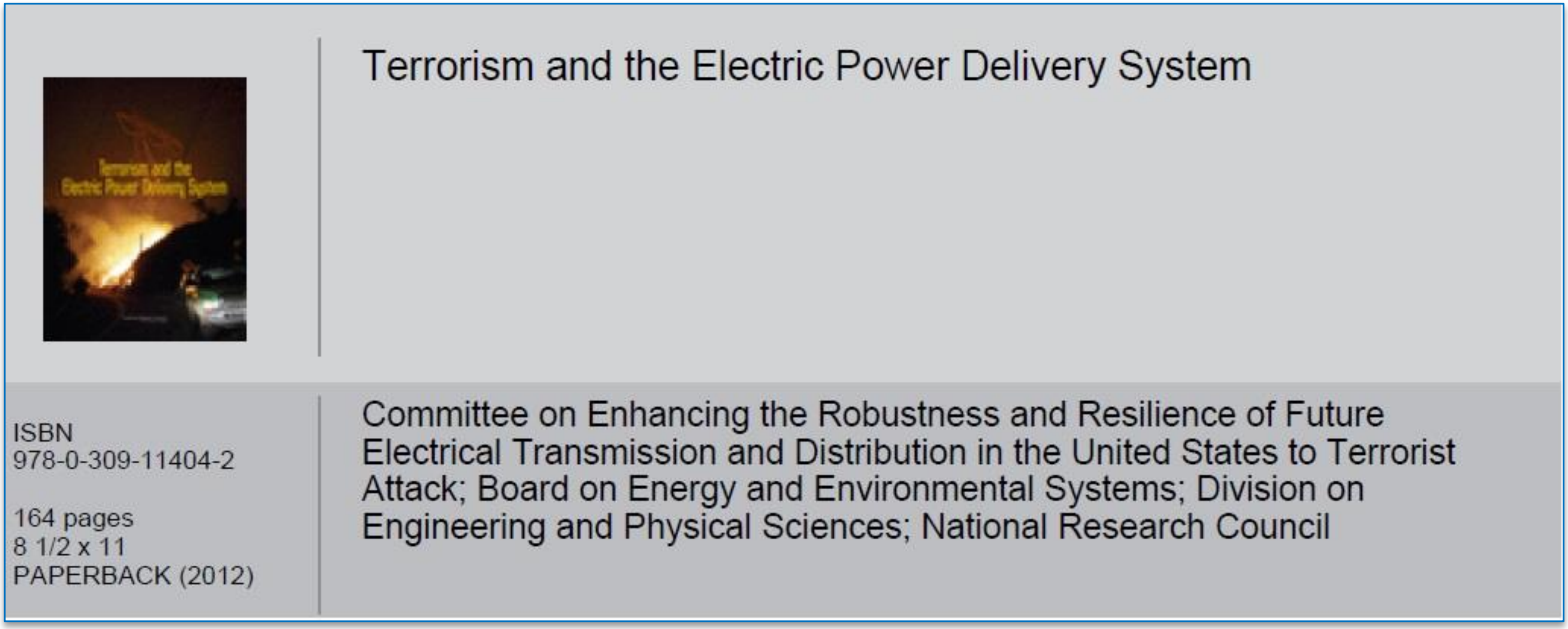
$b_1 \leftarrow a_1 + a_2 a_3$

$b_2 \leftarrow a_1 + a_3$

$b_3 \leftarrow a_1 a_2$

Entities	**Time Steps**						
	$\mathbf{t_1}$	$\mathbf{t_2}$	$\mathbf{t_3}$	$\mathbf{t_4}$	$\mathbf{t_5}$	$\mathbf{t_6}$	$\mathbf{t_7}$
a_1	1	1	1	1	1	1	1
a_2	0	0	0	0	1	1	1
a_3	0	0	1	1	1	1	1
a_4	0	0	0	0	1	1	1
b_1	0	0	0	1	1	1	1
b_2	0	0	0	1	1	1	1
b_3	0	1	1	1	1	1	1

Implicative Interdependency Model (IIM)



Terrorism and the Electric Power Delivery System

ISBN
978-0-309-11404-2

164 pages
8 1/2 x 11
PAPERBACK (2012)

Committee on Enhancing the Robustness and Resilience of Future Electrical Transmission and Distribution in the United States to Terrorist Attack; Board on Energy and Environmental Systems; Division on Engineering and Physical Sciences; National Research Council

This report focuses on measures that could:

1. Make the power delivery system less vulnerable to attacks,
2. Restore power faster after an attack,
3. Make critical services less vulnerable while the delivery of conventional electric power has been disrupted.

Implicative Interdependency Model (IIM)

Problems Studied using IIM (2014-2015)

❑ Identification of K Most Vulnerable Nodes in the Interdependent Networks
(Published in IEEE NetSciCom 2014, an Infocom Workshop)

❑ Root Cause of Failure Analysis
(Published in IEEE Milcom 2014)

❑ Progressive Recovery Problem
(Published in CRITIS 2014)

❑ Entity Hardening Problem in Networks
(Published in IEEE WIDN 2015, an Infocom Workshop)

❑ Smallest Pseudo Target Set Identification Problem
(Submitted to IEEE Milcom 2015)

❑ Robustness Analysis Problem
(Submitted to CRITIS 2015)

❑ Robustness Analysis with Incomplete or Incorrect Information
(Currently under study)

Prob. 1: Vulnerable Node Identification

- Problem: Identification of K most vulnerable entities in a multi-layered network.
- Definition: A set of entities in a multi-layered network is said to be the "most vulnerable" if failure of the K entities induces failure of the largest number of other entities in the multi-layered network.

"Identification of K most vulnerable nodes in multi-layered network using a new model of interdependency", A. Sen, A. Mazumder, J. Banerjee, A. Das, and R. Compton. Presented at NetSciCom 2014, 6th International Workshop on Network Science for Communication Networks held in conjunction with INFOCOM 2014.

An Example

Power Network

$$a_1 \leftarrow b_1 + \mathrm{b}_2$$
$$a_2 \leftarrow b_1 b_3 + b_2$$
$$a_3 \leftarrow b_3 b_1 b_2$$
$$a_4 \leftarrow b_1 + b_2 + b_3$$

Communication Network

$$b_1 \leftarrow a_1 + a_2 a_3$$
$$b_2 \leftarrow a_1 + a_3$$
$$b_3 \leftarrow a_1 a_2$$

Entities	**Time Steps**						
	t_1	**t_2**	**t_3**	**t_4**	**t_5**	**t_6**	**t_7**
a_1	1	1	1	1	1	1	1
a_2	0	0	0	0	1	1	1
a_3	0	0	1	1	1	1	1
a_4	0	0	0	0	1	1	1
b_1	0	0	0	1	1	1	1
b_2	0	0	0	1	1	1	1
b_3	0	1	1	1	1	1	1

Prob. 2: Root Cause of Failure

- Anatomy of Failures in Interdependent Networks:
  - Introduction of an *event-induced failure* in the system
    - Natural disasters (Hurricanes, Earthquakes), or terrorist attacks
  - Further *triggered failures* caused by *event-induced failures* due to the nature of interdependencies shared
  - Further *triggered-failures* caused by *event-induced* ***and*** *triggered failures* due to the nature of interdependencies shared
  - End of Cascade, no further failures in the system

- Objective of this study (Root Cause of Failure Analysis):
  - From the *final failure* set (*event-induced* + *triggered failures*) identify the original *event-induced* failure

"Root Cause Analysis of Failures in Interdependent Power-Communication Networks", A. Das, J. Banerjee, and A. Sen. Presented at MILCOM 2014, 33rd Military Communications Conference.

An Example

Power Network

$$a_1 \leftarrow b_1 + \mathrm{b}_2$$

$$a_2 \leftarrow b_1 b_3 + b_2$$

$$a_3 \leftarrow b_3 b_1 b_2$$

$$a_4 \leftarrow b_1 + b_2 + b_3$$

Communication Network

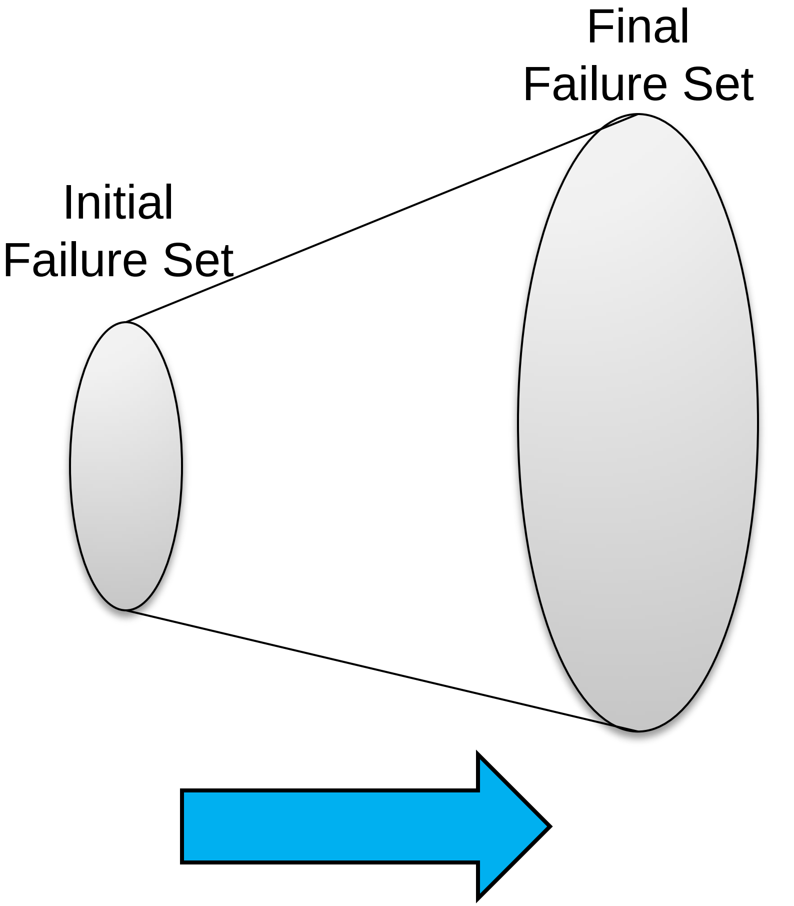
$$b_1 \leftarrow a_1 + a_2 a_3$$

$$b_2 \leftarrow a_1 + a_3$$

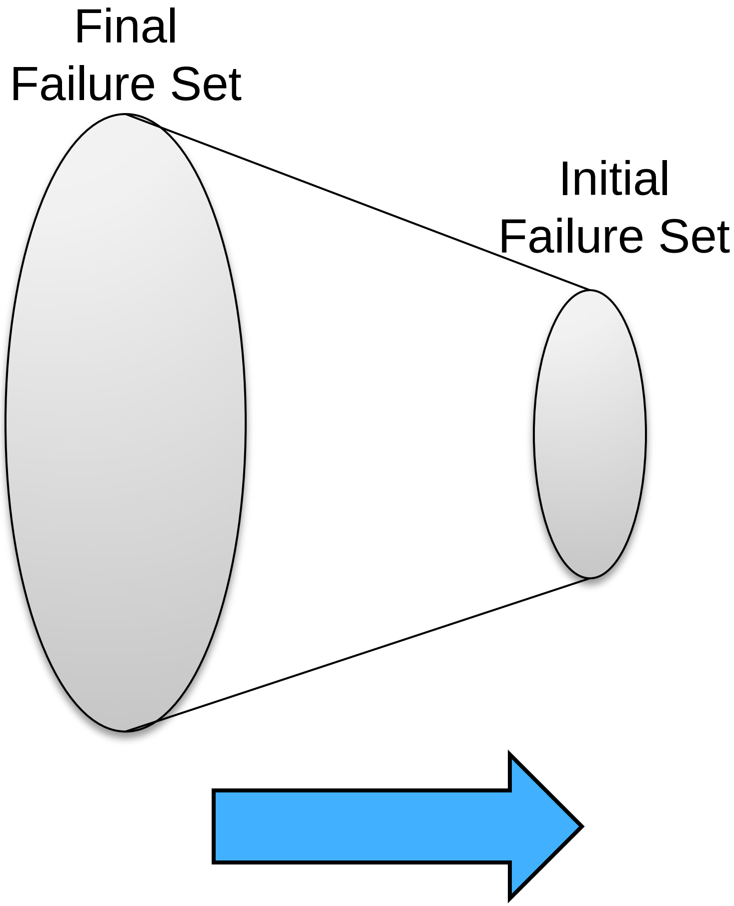
$$b_3 \leftarrow a_1 a_2$$

Entities	Time Steps						
	t_1	t_2	t_3	t_4	t_5	t_6	t_7
a_1	1	1	1	1	1	1	1
a_2	0	0	0	0	1	1	1
a_3	0	0	1	1	1	1	1
a_4	0	0	0	0	1	1	1
b_1	0	0	0	1	1	1	1
b_2	0	0	0	1	1	1	1
b_3	0	1	1	1	1	1	1

Vulnerable Node Identification vs. Root Cause of Failure



Vulnerable Node Identification Problem



Root Cause of Failure Problem

Prob. 3: Progressive Recovery Problem

- In an Interdependent Multi-layer Network System, failure of a set of A and B type entities initially (i.e. at time $t = 0$) can eventually lead to the failure of a much larger set of A and B type entities through the cascading failure process

- In order to take the system back to its original state all the entities that failed at time $t = 0$ must be repaired

- The entities can be fixed one after another in a sequential fashion

Prob. 3: Progressive Recovery Problem

- Just as failure of one entity can lead to the failure of another entity, fixing of one entity can lead to the fixing of another entity

- Fixing of one entity brings some “utility” value to the system
  - Failure of a number of power lines can cause a blackout to a large number of households. Fixing one power line can bring back power to some households.

- The sequence of fixing the originally failed entities will determine the system utility during the duration of the repair operation

Prob. 3: Progressive Recovery Problem

- Consider the following example of a set of IDRs:

Power Network	Communication Network
$a_1 \leftarrow \emptyset$	$b_1 \leftarrow a_1 a_2$
$a_2 \leftarrow \emptyset$	$b_2 \leftarrow a_1 + a_2$
…	$b_3 \leftarrow a_1$

- Failure of (a_1, a_2) leads to the failure of (b_1, b_2, b_3)

- In order to return the system to its normal operational state both a_1 and a_2 must be repaired

- Repair sequence could be (a_2, a_1) or (a_1, a_2).
  - Which repair sequence should be used?
    - Does it matter?

Prob. 3: Progressive Recovery Problem

- Whether a_1 is repaired first and then a_2, or the other way around, will have an impact on "system utility"

- Utility of an entity a_i, $\left(u(a_i)\right)$ is defined as the "benefit" obtained when the entity a_i is made operational

- $x_{a_i}(t)$: Indicator variable for entity a_i such that:

$$x_{a_i}(t) = \begin{cases} 1 & \text{entity } a_i \text{ is operational at time } t \\ 0 & otherwise \end{cases}$$

Prob. 3: Progressive Recovery Problem

- $SUIT(t)$: System Utility at Instance of Time t

$$SUIT(t) = \sum_{a_i \in V(A)} u(a_i) x_{a_i}(t) + \sum_{b_j \in V(B)} u(b_j) x_{b_j}(t)$$

- $SUOT(t)$: System Utility Over Time interval 0 to T

$$SUOT[T] = \sum_{t=0}^{T} SUIT(t)$$

- Example:
  - $u(a_1) = 10, u(a_2) = 10;$
  - $u(b_1) = 20, u(b_2) = 30, u(b_3) = 40$

Prob. 3: Progressive Recovery Problem

- Example:

Power Network	**Communication Network**
$a_1 \leftarrow \emptyset$	$b_1 \leftarrow a_1 a_2$
$a_2 \leftarrow \emptyset$	$b_2 \leftarrow a_1 + a_2$
…	$b_3 \leftarrow a_1$

- If the repair sequence is (a_2, a_1), then the system utility over time changes as follows
- Fixing of a_2 leads to fixing of b_2. Since $u(a_2) = 10$, and $u(b_2) = 30$

$$SUIT(1) = 10 + 30 = 40$$

- Now fixing a_1 leads to fixing of b_1, b_3. Since $u(a_1) = 10$, $u(b_1) = 20$, $u(b_3) = 40$

$$SUIT(2) = 10 + 30 + 10 + 20 + 40 = 110$$

Time step (t)	0	1	2
$SUIT(t)$	0	40	110
$SUOT[T]$	0	40	150

Prob. 3: Progressive Recovery Problem

- If the repair sequence is (a_1, a_2), then the system utility over time is as follows:

Time step (t)	0	1	2
$SUIT(t)$	0	80	110
$SUOT[T]$	0	80	190

- In this example the second sequence is preferable over the first
- Lesson learnt: Repair sequence matters!
- The goal of the progressive recovery problem is to identify the repair sequence such that the system utility over time $SUOT[T]$ is maximized

Prob. 3: Progressive Recovery Problem

- Problem statement:
  - Find the sequence in which the originally failed entities (i.e. the entities that failed at $t = 0$) should be repaired so that the total system utility is maximized

“Progressive Recovery from Failure in Multi-layered Interdependent Network Using a New Model of Interdependency”, A. Majumder, C. Zhou, A. Das, and A. Sen. To be presented at CRITIS 2014, 9th International Conference on Critical Information Infrastructures Security.

Prob. 4: Entity Hardening Problem

- Problem Domain: Adversarial Setting (Attacker-Defender Scenario)
- Adversary Knowledge: All the Dependency Relations that govern the system
- Adversary Intention: Cause maximum damage to the system (maximize inoperable entities)
- Adversary Resources: Adversary can render inoperable at most *K* entities of the system
- Adversary Action: Identify *K* most vulnerable nodes in the system

Prob. 4: Entity Hardening Problem

- If defender takes no action then the adversary will destroy *K* most vulnerable entities in the system that will cause maximum damage
- Entity Defense: Defender takes some action so that the attacker cannot destroy the entity
- If the defender has the resources to defend *K* entities then the attacker cannot inflict any damage to the system
- If the defender does not have resources to defend *K* entities, but say *K'* entities, where *K'<=K,* the defender has to decide which *K'* entities should be defended so that the impact of attack is minimized

Prob. 4: Entity Hardening Problem

- The *K'* entities that the defender decides to defend can no longer be rendered inoperable and will be considered as "Hardened" entities
- Entity Hardening problem is to identify the *K'* entities that should be defended by the defender so that impact of attack is minimized
- The implication of hardening an entity is a change in the set of dependency relations
- The dependency relations of the hardened entities can be removed from the set of dependency relations as these entities can no longer fail

Prob. 4: Entity Hardening Problem

- Assumption: The attacker is unaware of the action taken by the defender, i.e. how many entities, or which entities have been hardened
- As a consequence the attacker operates with the pseudo (original) set of dependency relations which may not be the real set of dependency relations that describes the system (after the hardening process)
- The goal of the entity hardening problem is to identify the set of *K'* entities whose hardening would minimize the impact of attack

Solution Approach

- Complexity Analysis of individual cases of dependency relations
  - Most general form of the dependency relation:

$$a_i \leftarrow b_j b_k b_l + b_m b_n + b_p$$

  - In the general form:
    - No. of Min-terms are arbitrary
    - Size of Min-terms are arbitrary
  - We consider four special cases for each problem:

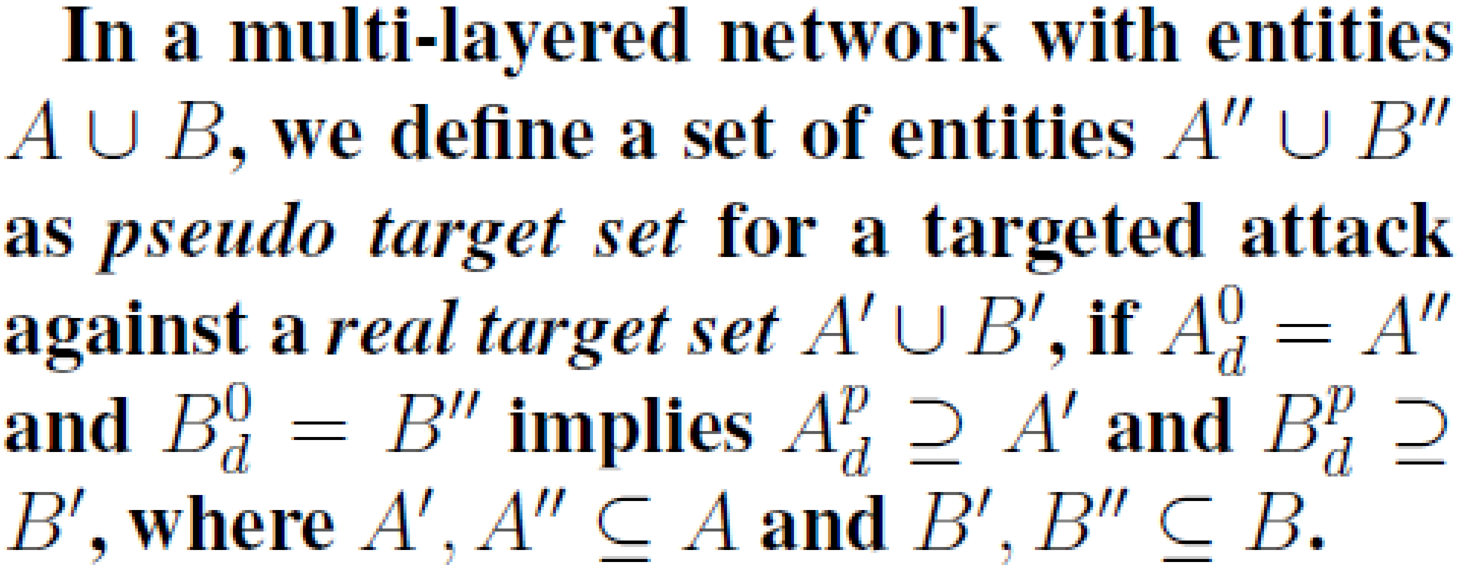
Case	No. of Min-terms	Size of Min-terms
Case 1	1	1
Case 2	Arbitrary	1
Case 3	1	Arbitrary
Case 4 (General)	Arbitrary	Arbitrary

Solution Approach

- Computation of optimal solution for each type of dependency relations
  - Using Integer Linear Programming (if NP-Complete)
- Development of a Approximate/Heuristic algorithm to compute solution for dependency relations proven to be NP-Complete
- Comparison of Optimal vs. Approximate / Heuristic approach with experimental results using both real and synthetic data

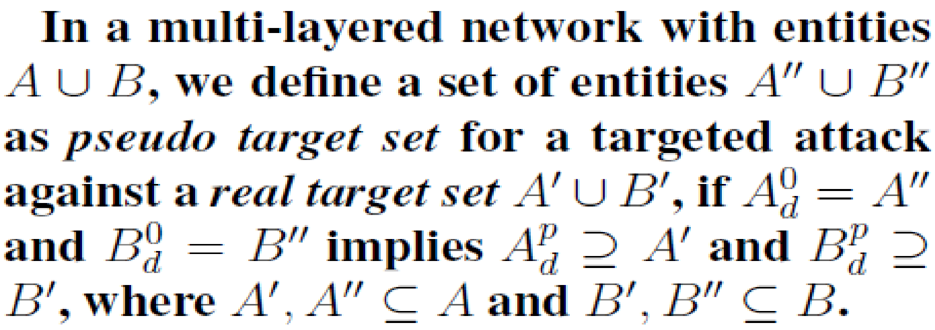
"On the Entity Hardening Problem in Multi-layered Interdependent Networks", J. Banerjee, A. Das, C. Zhou, A. Mazumder and A. Sen. Under review, Infocom 2015 Workshop on Inter-Dependent Networks (WIDN 2015).

Prob. 5: Smallest Pseudo-Target Set Identification Problem (STASIP) for Targeted in Interdependent Power-Communication Networks

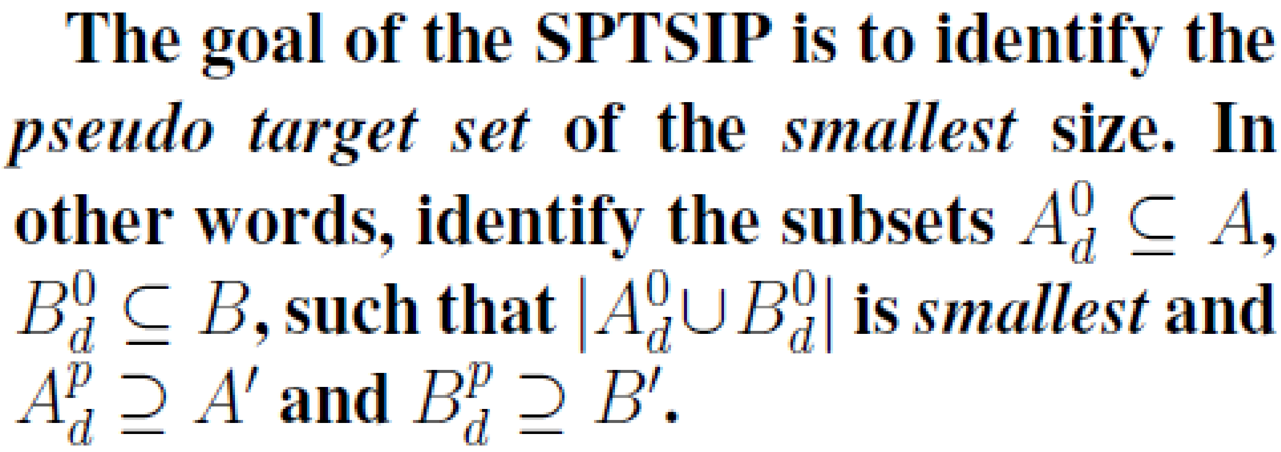


In a multi-layered network with entities $A \cup B$, we define a set of entities $A'' \cup B''$ as *pseudo target set* for a targeted attack against a *real target set* $A' \cup B'$, if $A_d^0 = A''$ and $B_d^0 = B''$ implies $A_d^p \supseteq A'$ and $B_d^p \supseteq B'$, where $A', A'' \subseteq A$ and $B', B'' \subseteq B$.

Prob. 5: Smallest Pseudo-Target Set Identification Problem (SPTSIP) for Targeted in Interdependent Power-Communication Networks



In a multi-layered network with entities $A \cup B$, we define a set of entities $A'' \cup B''$ as *pseudo target set* for a targeted attack against a *real target set* $A' \cup B'$, if $A_d^0 = A''$ and $B_d^0 = B''$ implies $A_d^p \supseteq A'$ and $B_d^p \supseteq B'$, where $A', A'' \subseteq A$ and $B', B'' \subseteq B$.



The goal of the SPTSIP is to identify the *pseudo target set* of the *smallest* size. In other words, identify the subsets $A_d^0 \subseteq A$, $B_d^0 \subseteq B$, such that $|A_d^0 \cup B_d^0|$ is *smallest* and $A_d^p \supseteq A'$ and $B_d^p \supseteq B'$.

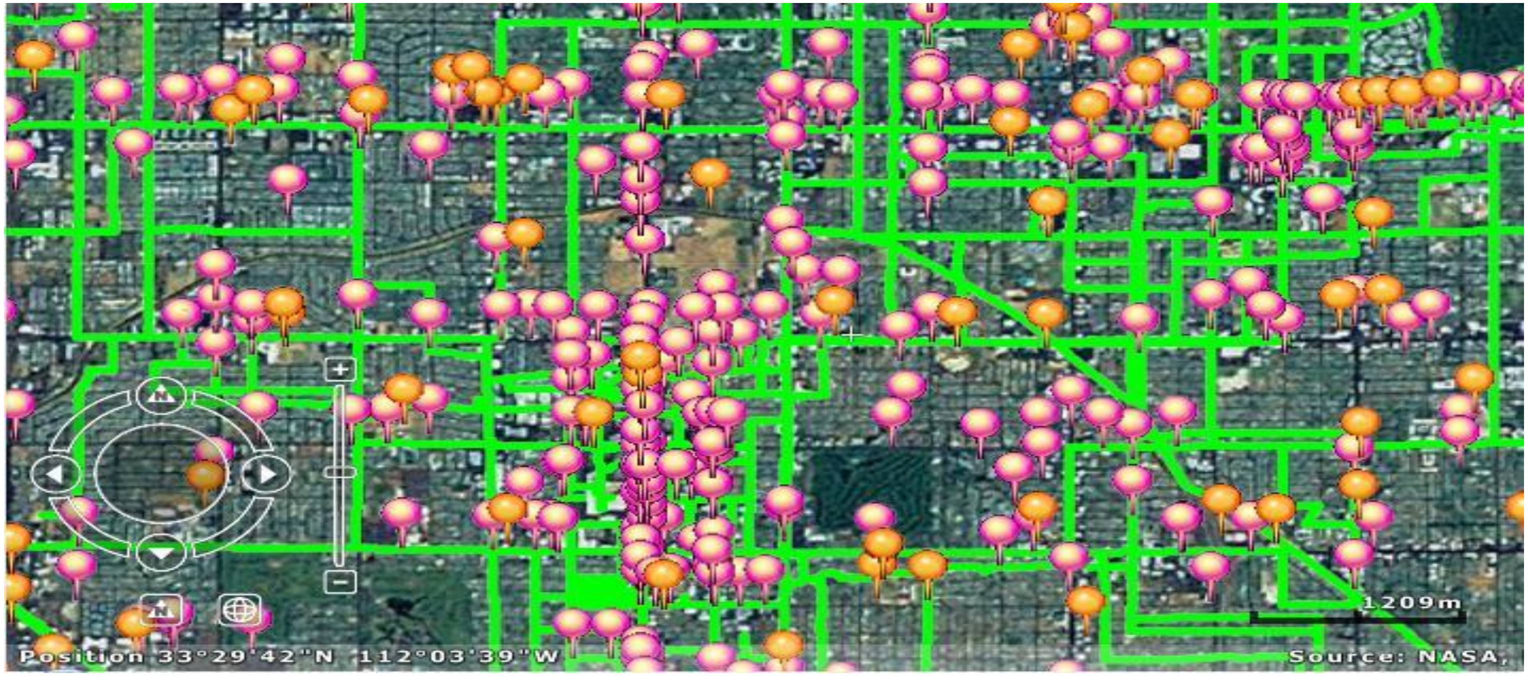
Prob. 6: Least Cost Robustness Enhancement

- Definition: Robustness Level of an interdependent network is measured in terms of the fewest number of entities whose failure will trigger failure of all (or a certain percentage) of the entities in the interdependent network

- The goal of the Least Cost Robustness Enhancement problem is to identify the way to take the network from Robustness Level X to Robustness Level Y, with least cost.

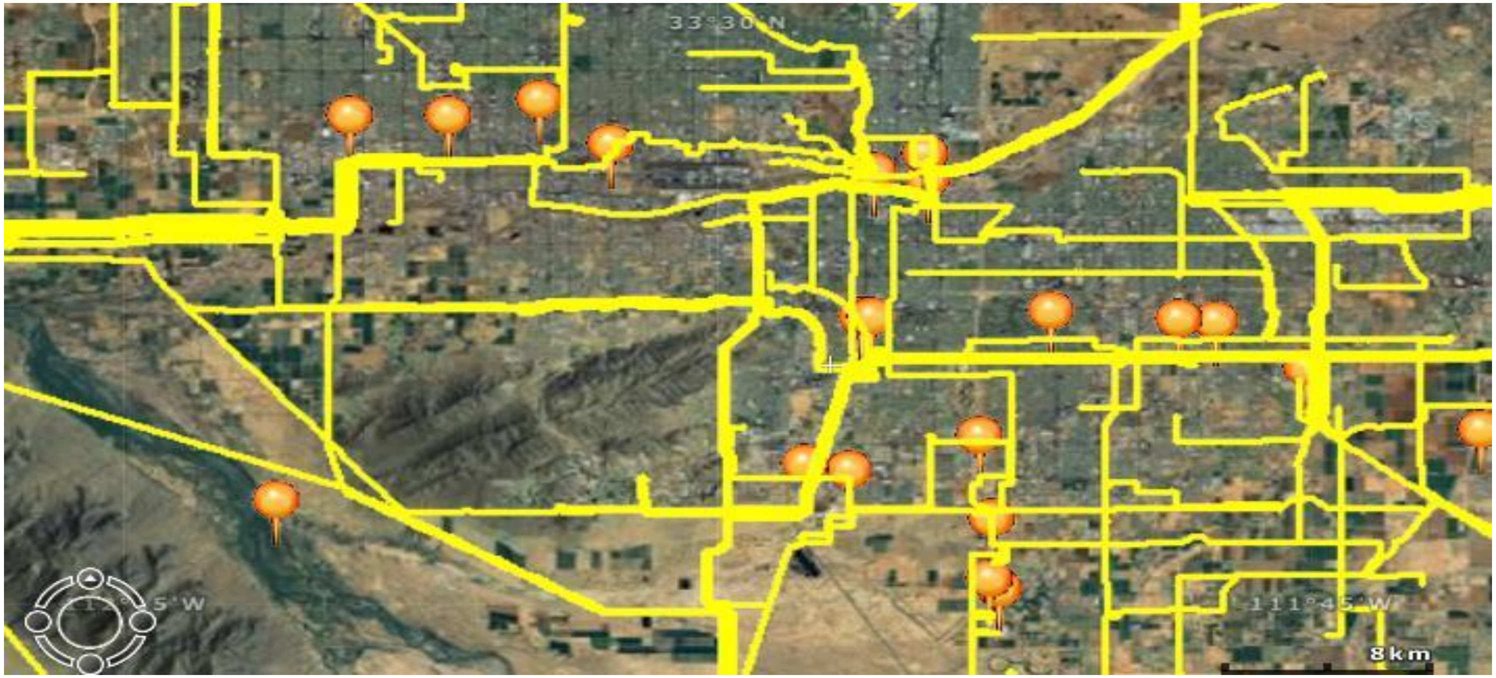
Experimental Data Sets

- Data Collection
  - CNE Data - Data of Cell Towers, Fiber Lit Buildings and Fiber Routes was collected from Geo-tel (http://www.geo-tel.com/) for Maricopa County.



Experimental Data Sets

- Data Collection
  - PNE data – Data of Power Plants and Transmission Lines was collected from Platts (http://www.platts.com/) for Maricopa County.



Experimental Data Sets

- Data from Maricopa County
- Power Network (PNE):
    - Power plants: 70, Transmission Lines: 470

- Communication Network (CNE):
    - Cell Towers: 2960, Fiber-lit building: 7100,
    - Fiber Links: 42,723

Future Directions

- Discovery of Dependency Relations
- Deterministic Dependency Relations vs. Probabilistic Dependency Relations
- Exploration of scale and granularity of entities for interdependent multilayer network analysis
- Generalization from Binary (operational/non-operational) state of entities to *n*-ary states
- Identification of robustness and resiliency metrics for interdependent networks
- Phasor placement problem taking into account interdependency between the networks

Future Directions

- **"Connected Component" Analysis:**
  - *Generalization of the concept of Connected Component of a Graph, $G = (V, E)$ (single layer), to Multi-layer Interdependent Network $(G_1, G_2, \ldots, G_m, R)$*
- **"Islanding" in Multi-Layer Networks**
  - *Generalization of the concept of an "island" in a power network, $G = (V, E)$ (single layer), to a Multi-layer Interdependent Network $(G_1, G_2, \ldots, G_m, R)$*

Thank You!