Institute for Infrastructure Surety

IFIS

www.ece.unm.edu/ifis

Professor Edl Schamiloglu
Director
Department of Electrical and Computer Engineering
University of New Mexico
Albuquerque, NM 87131
505/277-4423
edl@ece.unm.edu

The Need for this Institute

"The increasing complexity and interconnectedness of energy, telecommunications, transportation, and financial infrastructures pose new challenges for secure, reliable management and operation.[1]"

"Complex interactive networks are omnipresent and critical to economic and social well-being.[1]"

[1] M. Amin, "National Infrastructures as Complex Interactive Networks," Chapter 14 in *Automation, Control, and Complexity: An Integrated Approach*, T. Samad and J. Weyrauch, Eds. (John Wiley and Sons, NY, 2000).

The Need for this Institute

- *The University of New Mexico* has a critical mass of creative and talented faculty and research staff that have been working on many aspects of these problems with their students for over a decade.

- *The University of New Mexico* is unique in that, it not only has faculty and research staff that cover the breadth of research in complex interactive networks, but it also has faculty and research staff that possess depth in research into the modeling and control of networks, and several specific threats to networks.

- *The University of New Mexico* is forming the Institute for Infrastructure Surety in order to pool its talent and resources to work on this problem that is important to the State of New Mexico, as well as the Nation.

The Complex Nature of this Multidisciplinary Problem

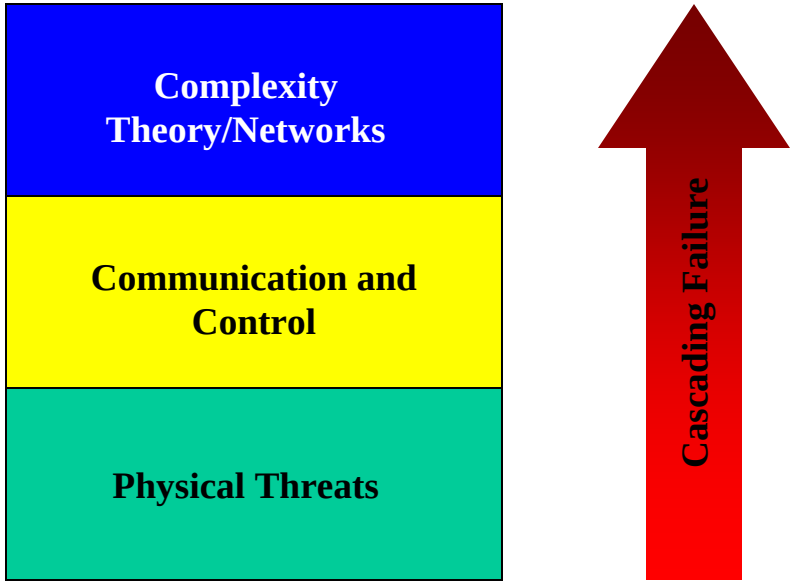
We view infrastructure surety as involving three layers:

At the *lowest layer*, we consider specific physical threats to individual assets that might be stationary (such as a power plant that is part of a larger electric grid) or might be mobile (robotic sensors).

At the *middle layer*, we consider communication and control within a network.

At the *highest layer*, we consider more complex interactions, such as networks within networks. It could also involve the effects of social networks as well.

The Complex Nature of this Multidisciplinary Problem



Our Vision for the Institute

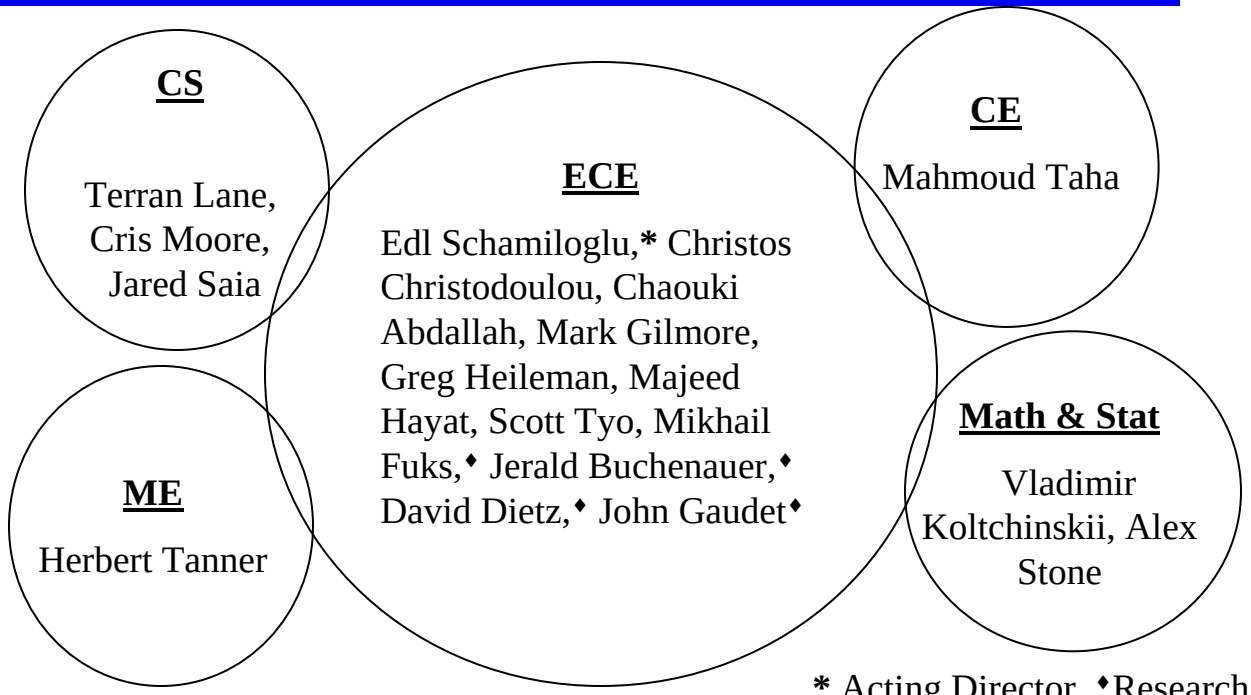
The Institute was founded in the Summer 2004 by faculty in The University of New Mexico Department's of Electrical & Computer Engineering, Computer Science, Mechanical Engineering, Civil Engineering, and Mathematics & Statistics who decided to pool their talents and resources to address a shared concern: threats to the civilian infrastructure and their mitigation.

The University of New Mexico

Faculty Affiliated with The Institute

IfIS

Institute for Infrastructure Surety



* Acting Director, ♦Research Faculty

Institute unites experts in High Power Electromagnetics, RF Effects, Wave Chaos and Statistical EM, Complexity Theory, Communication and Control Theory, Probability Theory, and Network Analysis & Optimization

What Motivated us to Launch this Institute?

Although we have been working on various aspects of this problem across the School of Engineering and with colleagues in Arts & Sciences, the awarding of the *DTRA University Strategic Partnership Program* has provided the impetus to found this Institute.

The University of New Mexico

IfIS

DEFENSE THREAT REDUCTION AGENCY

DTRA

Making the World Safer

DTRA Strategic Themes

University Strategic Partnership Program 2003

The University of New Mexico

IfIS

Blue Team

Applied Research Laboratory at
Pennsylvania State University (Prime)

University of California at San Diego
University of Florida
Florida A & M *
North Carolina A & T *
New Mexico Institute for Mining and Technology
Pennsylvania State University

* Indicates HBCU/MI

Gold Team

University of New Mexico (Prime) *

New Mexico State University *

* Indicates HBCU/MI

Electromagnetic Attack to Systems and Critical Infrastructure*

UNM
- Schamiloglu (PI)
- Christodoulou
- Tyo
- Gaudet

+ Giri and Tesche

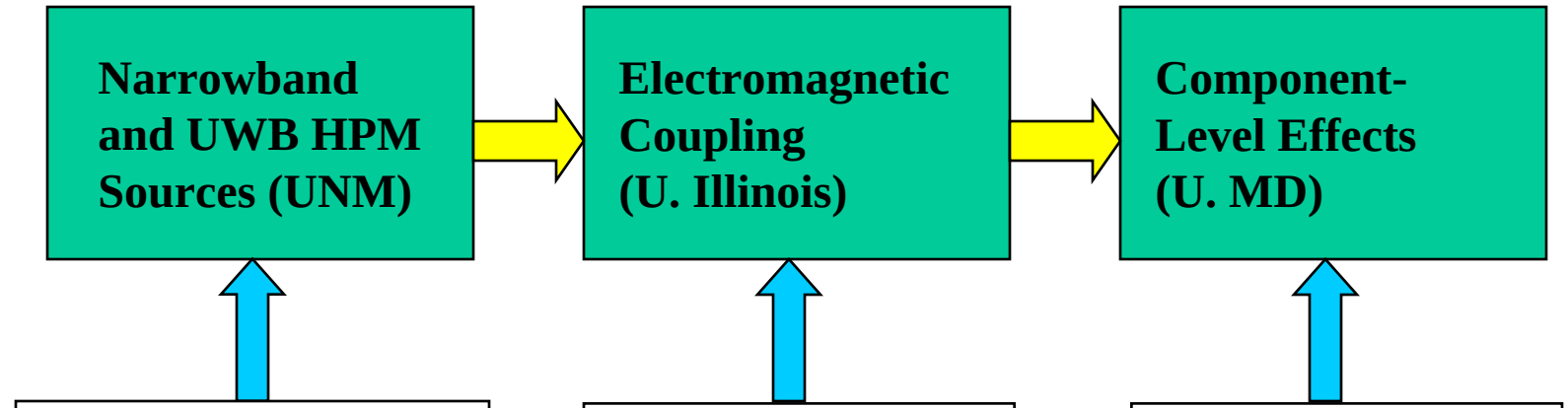
NMSU
- Jedlicka
- Blevins (PSL)

Physical Threats

Electromagnetic Attack Addresses the Lowest Layer

** Program began July 2004.*

The Lowest Layer: Electromagnetic Attack – Existing University Programs in the U.S.



The University of New Mexico

Collaborating Organizations (to-date):

IfIS

Institute for Infrastructure Surety

- The University of Maryland
- Air Force Research Laboratory/DEHE
- Los Alamos National Laboratory
- Ohio State University
- New Mexico State University
- Sandia National Laboratories' NISAC (National Infrastructure Simulation Analysis Center)
- New Mexico Office of Homeland Security

Institute for Infrastructure Surety

Sampling of Research Interests of other UNM Institute Participants:

The University of New Mexico

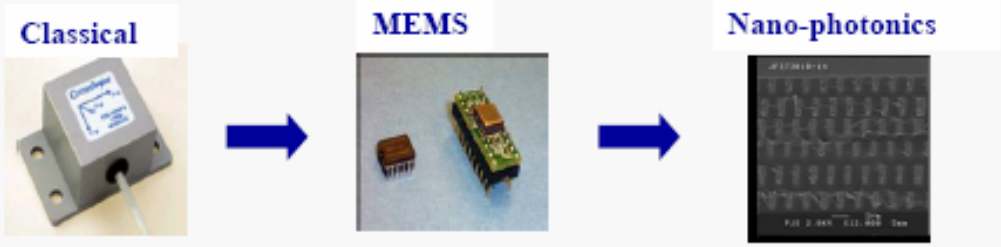
Physical Threats

Professor M.M. Reda Taha,
Civil Engineering

IfIS

Intelligent Structural Health Monitoring of Civil Infrastructures

- Develop ***robust sensing techniques*** to provide efficient ***mutli-scale*** damage detection in infrastructures.



- Investigate the fundamental processes for developing a reliable ***intelligent damage diagnostic module***.

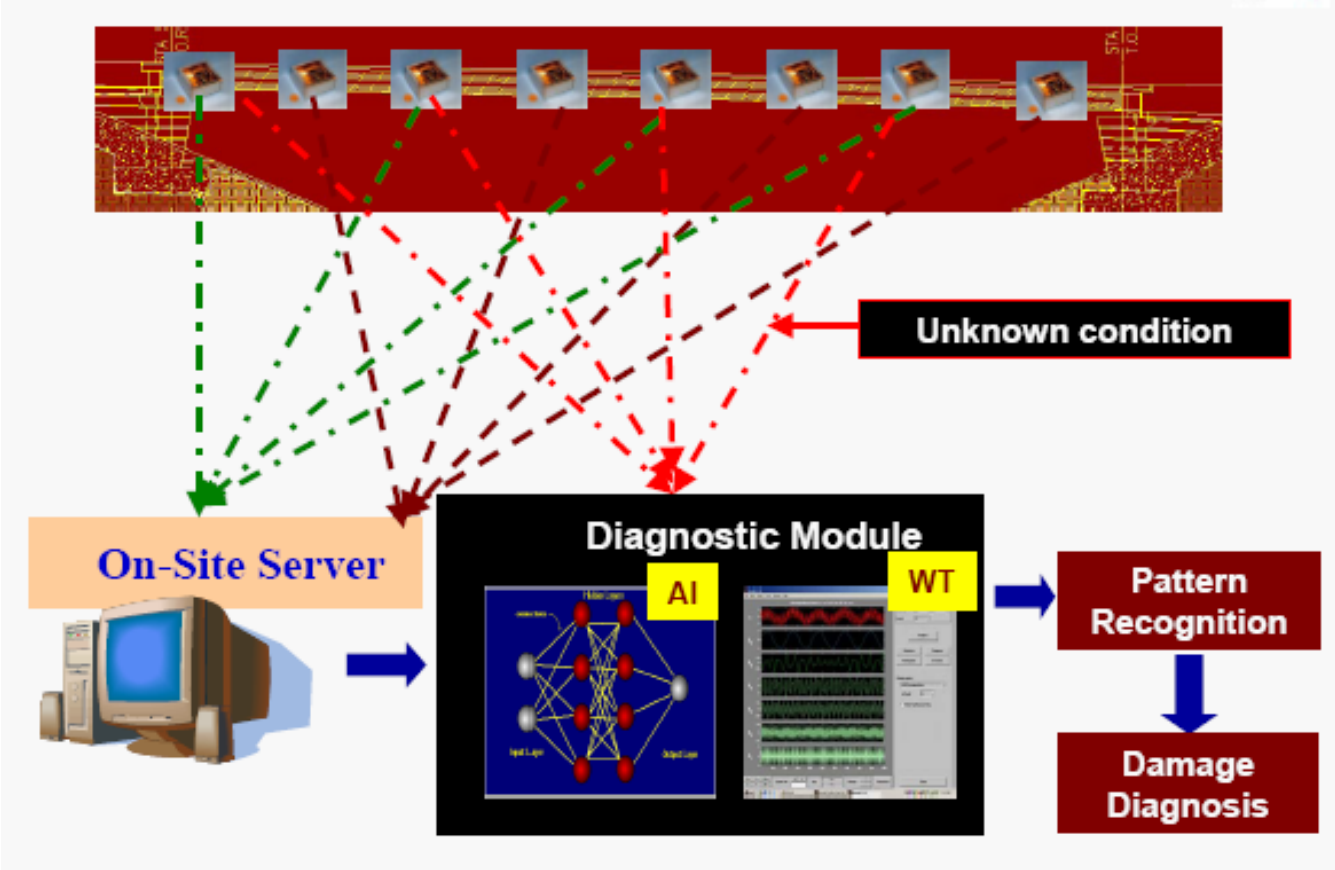
- Investigate ***structural surety*** through examining the primary techniques ***to relate*** the possible ***in-situ*** structural health condition to the level of structural ***safety and reliability***.

The University of New Mexico

Professor M.M. Reda Taha,
Civil Engineering

IfIS

Intelligent Damage Diagnosis Research

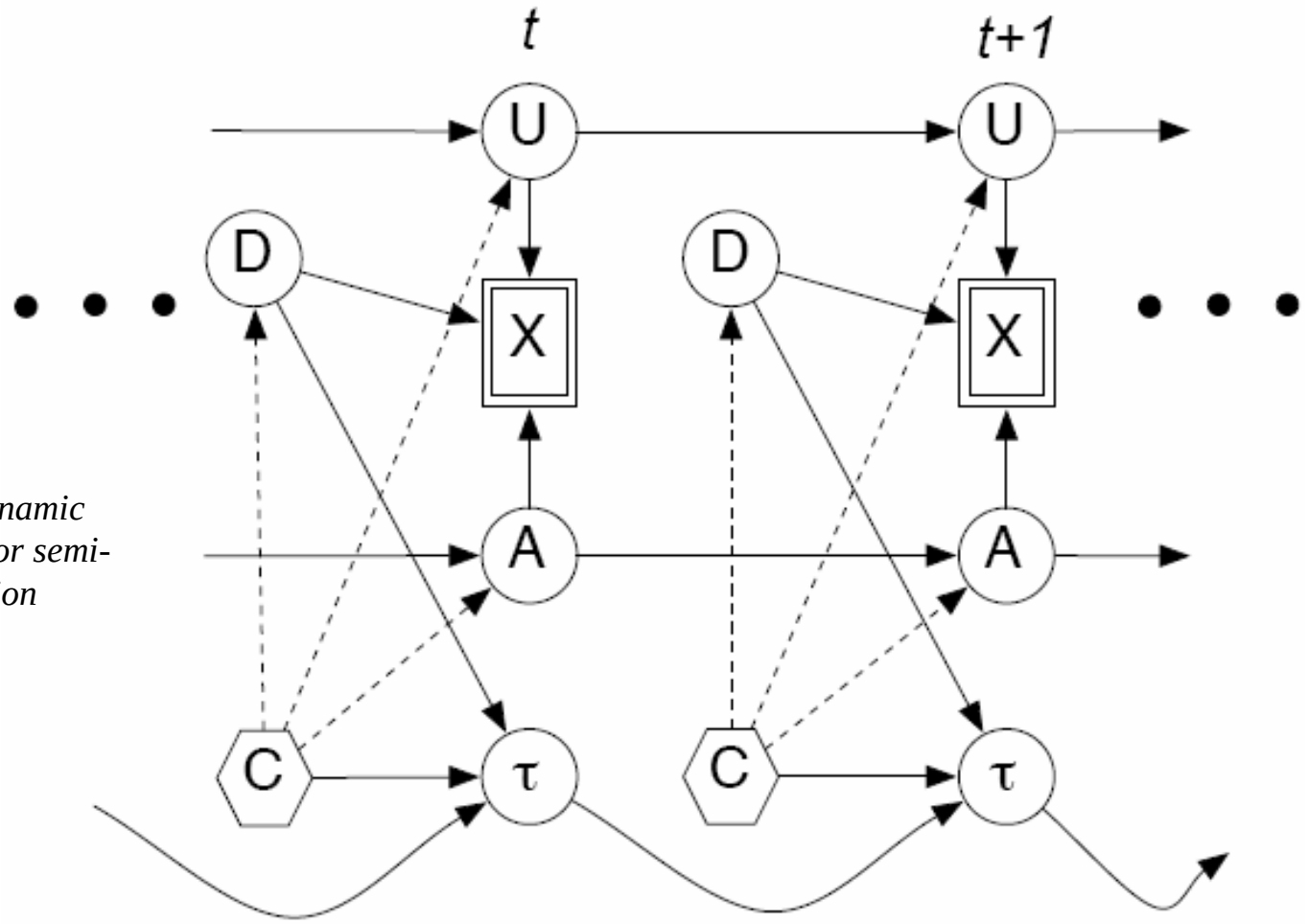


The University of New Mexico

Complexity Thy/Network.

Professor Terran Lane, Computer Science

IfIS



The figure represents a dynamic Bayesian network model for semi-supervised network intrusion detection.

October 7, 2004

Professor Terran Lane,
Computer Science

Related Interests:

• **Anomaly and intrusion detection:** Detecting unusual or hostile occurances in individual hosts and in distributed network systems.

• **Sensor fusion:** Integration of knowledge from multiple, networked sensors into a holistic view of system status and environmental conditions.

• **Network identification:** Identifying the presence and structure of causal activity networks in complex, probably nonlinear, high-dimensional data.

• **Methods:** Machine learning; statistical decision theory; Bayesian time series modeling; relational network modeling; network structure scoring and search.

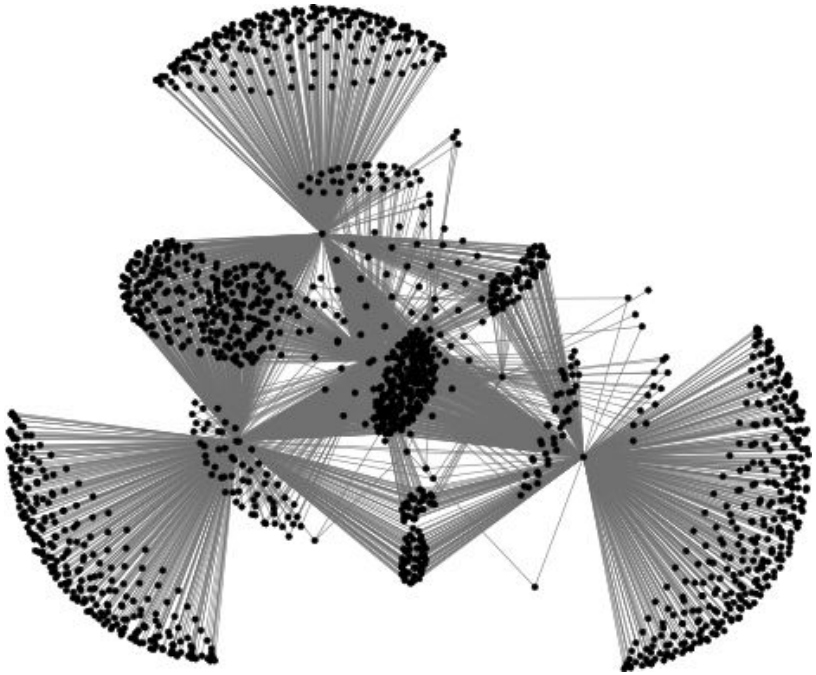
The University of New Mexico

Complexity Thy/Network.

Professor Cris Moore, Computer Science (and Physics & Astronomy)

IFIS

Research Interests Relevant to IFIS:



- **Community structure in networks**

The figure represents a visualization of the community structure at maximum modularity. Some major communities have a large number of "satellite" communities connected. Highly connected nodes are more critical to a network.

- **Scaling of the Internet topology, computational complexity in statistical physics, social networks, and "Small Worlds."**

The University of New Mexico

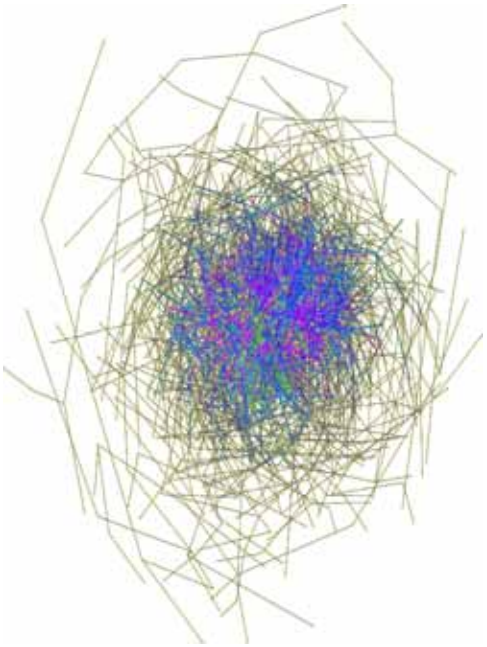
Complexity Thy/Network.

Professor Jared Saia, Computer Science

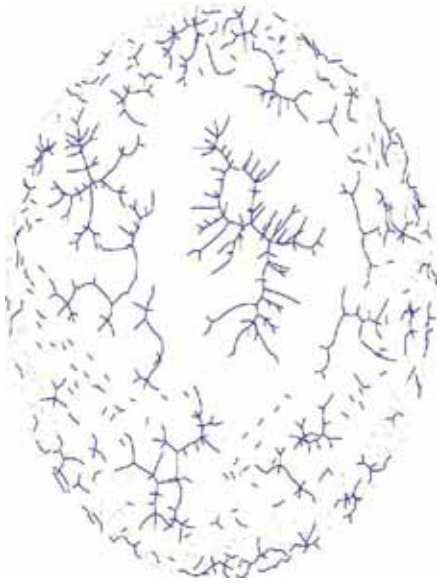
IfIS

Networks are Vulnerable

- Many current networks are robust to random faults
- However, they are not robust to adversarial faults



Pre-attack



Post-attack: attack deletes just 63 nodes, but the network has been shattered into a large number of small connected components.

The University of New Mexico

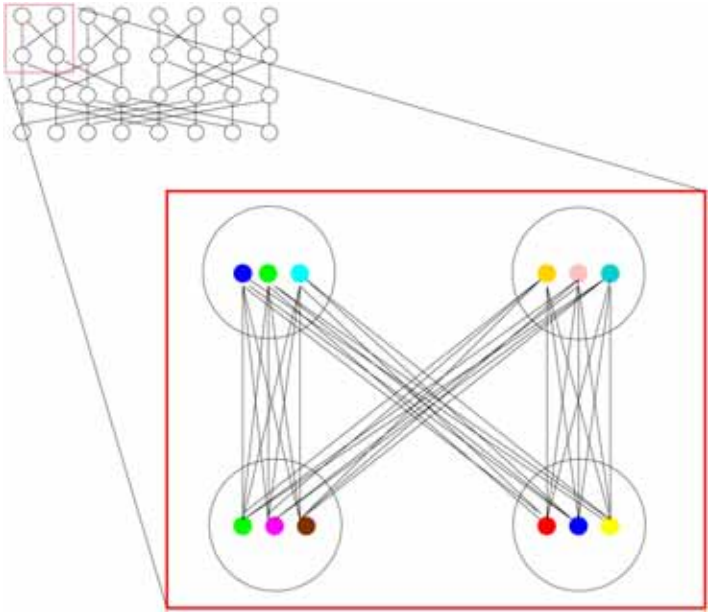
Professor Jared Saia,
Computer Science

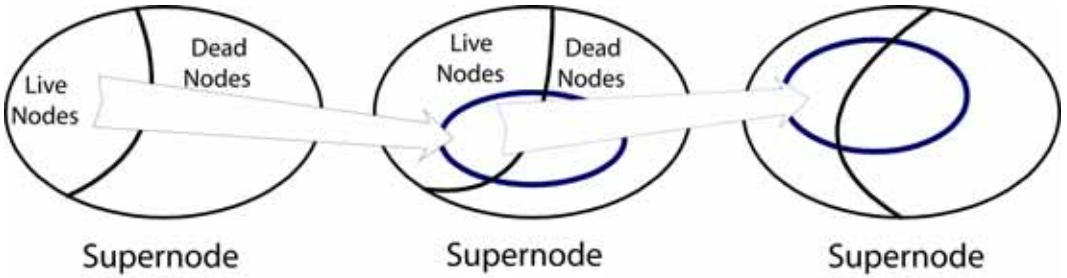
IfIS

Defending Networks

Result: Network which will function even after massive adversarial attack
- Network is robust after adversarial deletion of nodes
- Network is robust after adversarial control of nodes

Key Ideas:
- Nodes collaborate to form robust functional units called “Supernodes”
- Supernodes are connected in robust topology





The University of New Mexico

Communication and Control

Professor Chaouki Abdallah,
Electrical & Computer Engineering

IfIS

- **Networked Control Systems:** collaborative work with the University of Illinois to teleoperate networked robots.
- **Distributed Computing:** collaborative work with the University of Tennessee on load balancing across a network of computers.
- **Congestion Control:** This work is in collaboration with colleagues in Europe to combine congestion controllers on the Internet with real-time controllers for robotic systems.

Professor Chaouki Abdallah,
Electrical & Computer Engineering

- **Complex Networks Research:** We are also interested in studying the survivability, navigability, and robustness of networked systems, especially as they relate to wireless sensor networks and networked control systems. (This work is partially funded by Sandia National Laboratories, and AFOSR.)

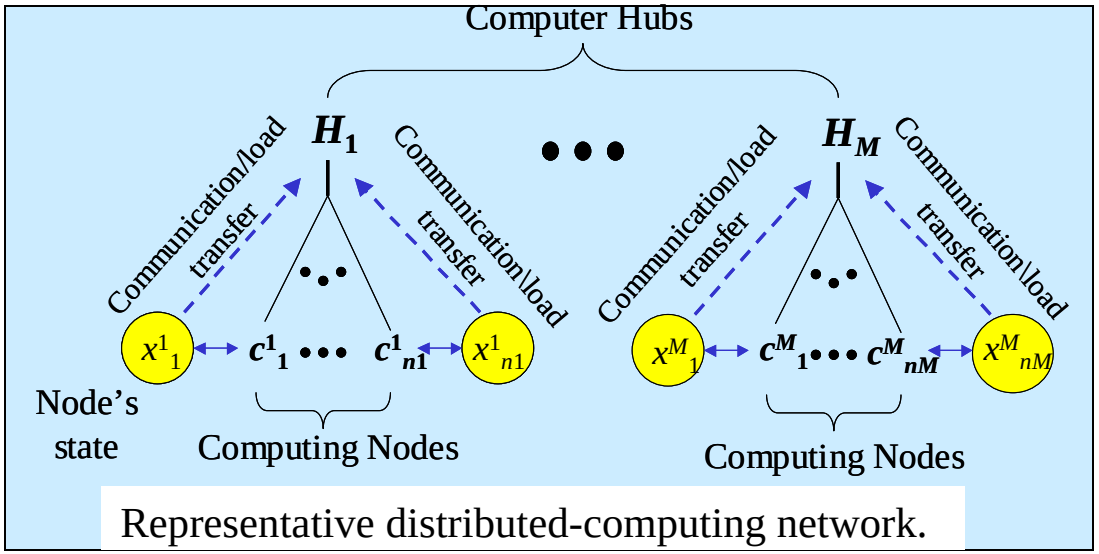
The University of New Mexico

Communication and Control

Professor Majeed Hayat,
Electrical & Computer Engineering

IfIS

Modeling and Optimization of Resource Sharing in the Presence of Large, Random Communications Delays



Representative distributed-computing network.

October 7, 2004

Professor Majeed Hayat,
Electrical & Computer Engineering

- In mobile wireless networks, reconfigurable networks, and networks with nodes that are geographically-distant, communication and load-transfer delays play a significant role in the collective performance of heterogeneous distributed systems over such networks.
- Incurred delays are large and random (unpredictable).
- This leads to dated, unreliable knowledge of each node about the state of other nodes and the state of the network; effective autonomous resource sharing and management becomes a challenge.
- ***Key problem:*** Standard resource-sharing policies perform poorly (possibly catastrophically) in such random-delay-infested environments.
- ***Ongoing research funded by NSF (ITR Program):*** Probabilistic modeling (analytical and Monte-Carlo based), performance assessment (theoretical and experimental), and development of optimized resource-sharing policies that mitigate the adverse effects of random delay. Significant performance enhancement and robustness can be achieved.
- ***Other issues under investigation:*** Effects of bandwidth and node/link failure; power-usage constraints and optimization in distributed resource-sharing environments.

The University of New Mexico

Complexity Thy/Network.

Professor Greg Heileman,
Electrical & Computer Engineering

IfIS

The data assets that exist and are shared across complex networks in order to make them available are highly vulnerable to various threats due to this availability. These include:

- Malicious destruction – network users may use their access privileges in order to modify or destroy data resources attached to the network.
- Insider threat – trusted people/computers/networks that have preferential access to confidential data may apply their privileges in order to misuse the data.
- Uncontrolled distribution – certain applications require the ability to distribute data or content to a select group; however, once data are provided to users, how do you prevent them from distributing the data further?

The Insider Threat Problem

- Applications of machine learning techniques to determine the type, level, and granularity of security to be applied in real-time to particular document objects.
- Includes an investigation of the types of forensic evidence that can be inserted in order to augment security and address insider threat scenarios.
- Involves categorization of content security levels from a rigorous perspective, allowing specific assurances to be made regarding software-only, hardware-assisted, and networked security solutions involving trusted third parties.

The University of New Mexico

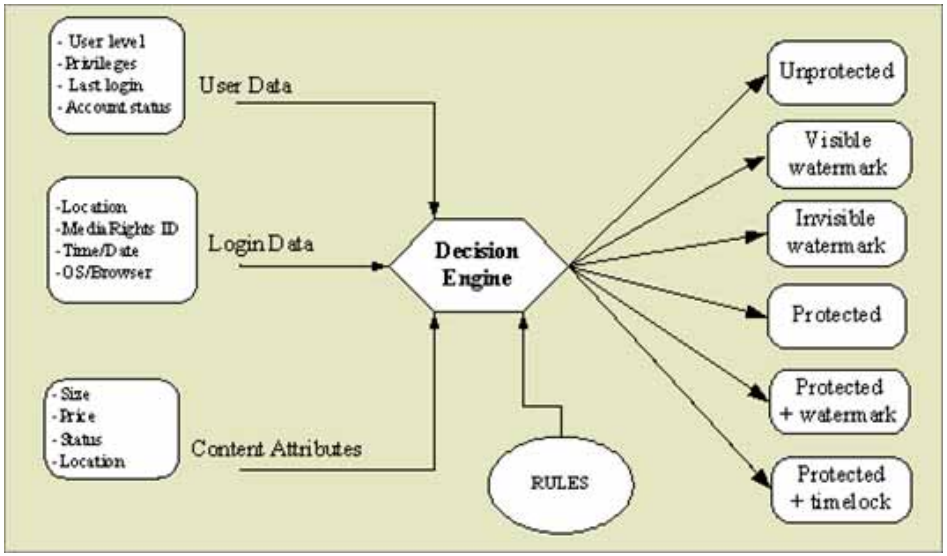
Complexity Thy/Network.

Professor Greg Heileman,
Electrical & Computer Engineering

IfIS

Uncontrolled distribution

- Controlling how the data assets within a networked environment are manipulated falls under the area of digital rights management (DRM), and also applies to the insider threat problem.
- DRM is an emerging field attempting to address electronic distribution problems in the entertainment industry, but the technologies involved apply equally to networks supporting data belonging to corporate, government, or military entities.
- As yet, the techniques/technologies capable of providing this functionality are very immature. A specific system we have developed is depicted below:

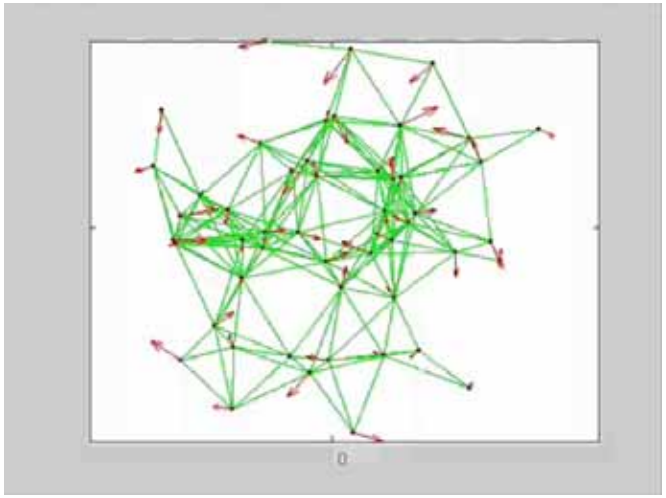


The University of New Mexico

Communication and Control

Professor Herbert Tanner, Mechanical Engineering

IfIS



Biological systems inspire control algorithms for synchronization in mobile networks

Networks have “natural” coordinating leaders that can be identified by studying the network topology. Leaders are critical network components that have to be safeguarded agains attacks

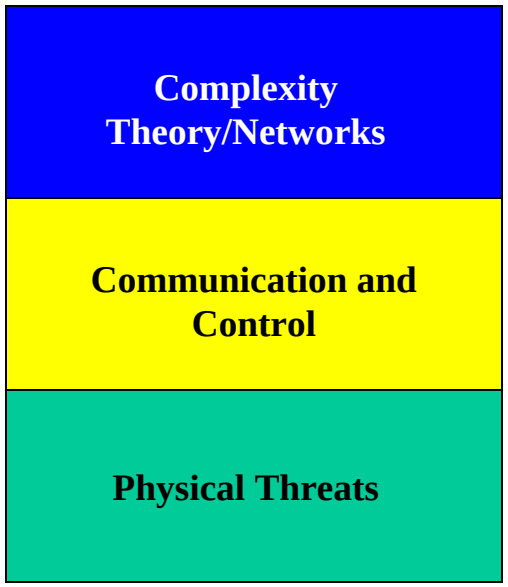
(Group leader shown as a **green** circle)

The Institute's Focus is Unique

GOALS

i) Study Specific Physical Threats to the Civilian Infrastructure
ii) Assess Vulnerability to Cascading Failure
iii) Mitigate Threats

TOOLS



RESULTS

The University of New Mexico