

# Network Forensics and Security

Pierre Moulin

University of Illinois at Urbana-Champaign

Electrical and Computer Engineering

NSF Workshop

Monitoring/Controlling the Nation's Critical Infrastructure

November 17, 2006

## My Background

- Statistical signal/image modeling and processing
- Detection and estimation theory
- Information theory and statistics
- Game theory and security
- EIC of IEEE Trans. on Information Forensics and Security

## Challenges

- **Network forensics:**  
detection and characterization of anomalous network events
- **Network security:**  
resistance to jammers, eavesdroppers
- **Critical networks include**
  - computer networks, e.g., Internet
  - (environmental, biological, ...) sensor networks
  - (audio, image, video, ...) surveillance systems
  - power grid
- **Challenges:** system and event modeling, information representation and extraction, reliability analysis

## (Top-Down) Research Issues

- **modeling** of network, anomalous events, and adversaries
- **design** of network, sensors, control & feedback mechanisms
- **complexity** of communication/control protocols
- **tradeoffs**, e.g., forensics *vs* privacy
- **performance metrics** (risk, delay, complexity, sensitivity)
  
- **enabling technologies**: stochastic processes, dynamical systems, randomization, cryptography, signal processing, decision theory, game theory, information theory, learning theory

## Strategic Issues (breakthroughs needed)

- efficient information representation and extraction
- coping with very large datasets:  
compression, search engines, queries (feedback)
- resistance to jammers, eavesdroppers
- (model-based) fundamental performance limits
- model validation, robustness, adaptivity