Computational Models of Systems Resilience and Application on Cybersecurity
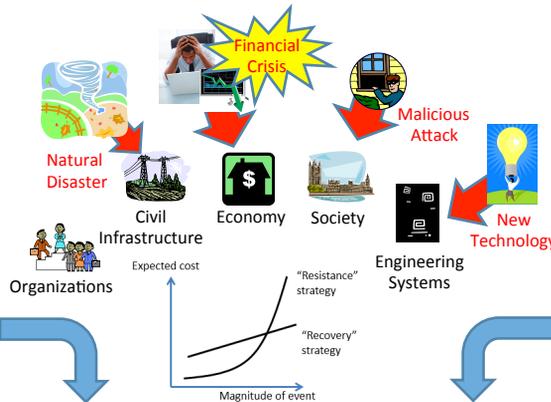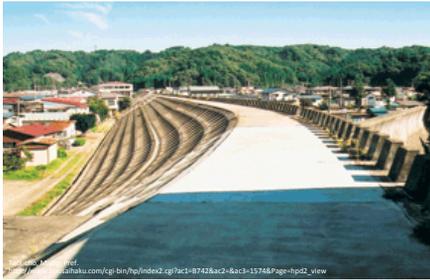
Hei Chan
Assistant Professor, Transdisciplinary Research Integration Center

Systems Resilience
Project of Transdisciplinary Research Integration Center

Goal: How to make our systems more resilient against large perturbations?

Natural Disaster · Civil Infrastructure · Economy · Society · Engineering Systems · Organizations · Financial Crisis · Malicious Attack · New Technology

Expected cost · "Resistance" strategy · "Recovery" strategy · Magnitude of event

Abstraction of problems: SR-Model
- Mathematical foundations/models
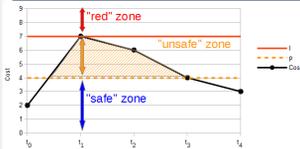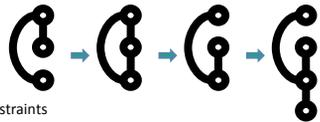- Symbolic representation (Artificial Intelligence)

Design of resilient systems:
- Uncertainty
- Robustness analysis
- Dynamic models

SR-Model

SR-Model (Schwind *et al.*, AAMAS 2013)
- Dynamic systems
- Multi-agent systems
- Constraint-based systems
- Flexible, can add/delete agents/constraints

"red" zone · "unsafe" zone · "safe" zone

Resistance + Recoverability = Resilience

Summary:
- Several properties to characterize the resilience of dynamic systems (*l-resistance*, <p,q>-recoverability, *f*-functionality, *s-stabilizability*)
- Very important framework for the design of "robust" dynamic systems in many fields

Open problems:
- **Theoretical complexity**: given a dynamic system and some fixed parameters l, p, q, f, s, does our dynamic system satisfy all properties listed above?
- **Optimization problems**: if our dynamic system must be f-functionable and s-stabilizable, how recoverable can it be?

Related Publications:
Nicolas Schwind, Tenda Okimoto, Katsumi Inoue, Hei Chan, Tony Ribeiro, Kazuhiro Minami, Hiroshi Maruyama: "Systems Resilience : a Challenge Problem for Dynamic Constraint-Based Agent Systems". In Proceedings of the 12th International Conference on Autonomous Agents and Multi-Agent Systems (AAMAS 2013), pp. 785-788 (**Challenges and Visions Papers 3rd prize**).


Robustness Analysis of Dynamic Models

Summary:
- **Uncertainty:** Some information of the system configuration may be uncertain
- **Robustness Analysis:** Study how outputs of model change given perturbations (e.g., environmental changes, unexpected events, estimation errors) in inputs of model
- **Dynamic Models:** Represent systems that evolve over time due to actions and/or external events

Relevance to Resilience:
- Check whether conclusions drawn from model are robust against perturbations
- Determine whether changes in system design improve system robustness
- Make tradeoffs between robustness and functionality

T = 1 · T = 2 · T = 3
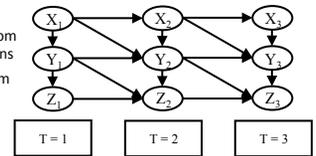
Relevance to System Design:
- For model builders, who design and debug models: What are the "weak" points of model that may contribute to large variations in output? What components we can change to improve model robustness?
- For decision makers, who use and evaluate models: What are the causes of certain decisions being made based on the model? How confident are we in the decisions against uncertainty?

Related Publications:
- Hei Chan, Sensitivity Analysis of Probabilistic Graphical Models, Verlag-Muller, 2009.

Example: Bayesian networks

Summary:
- Bayesian networks can be used to model uncertain and dynamic systems
- For robustness analysis, compute derivatives of probabilities of interest w.r.t. parameters
- Find solutions where parameter changes can enforce query constraints
- Experts can make guarantees of systems resilience in the face of unexpected events, or whether changes in system design will affect current conclusions

---
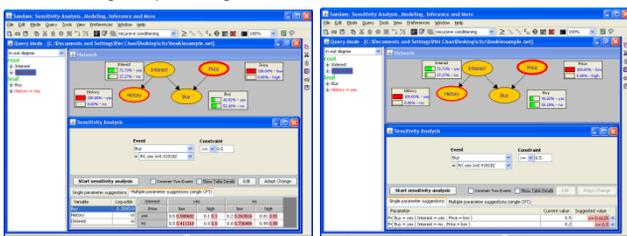
Application: Cybersecurity

Summary:
- A set of devices (servers, laptops, tablets) must work to provide service to citizens
- Hackers try to attack units to bring down service
- Administrators take actions (upgrade, fix) to keep devices working

Hacker · Attack · Administrator · Operate / maintain · Provide Service · Citizens

Immune · Upgrade · Vulnerable · Fix · Attacked

大学共同利用機関法人 情報・システム研究機構
統計数理研究所

The Institute of Statistical Mathematics