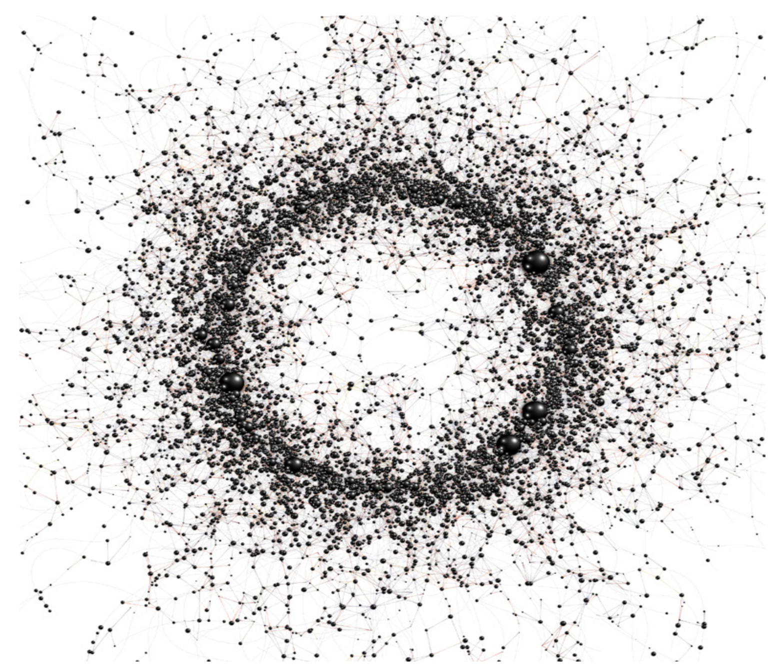
Efficient Information Spread Control in Cyber-Physical Systems

Ali Khanafer and Tamer Başar
Coordinated Science Laboratory, ECE, University of Illinois at Urbana-Chamapign

Networks in CPS

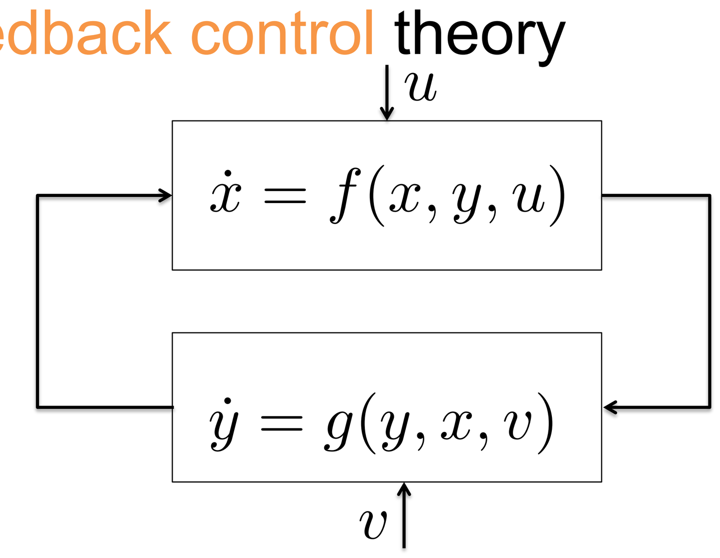
- Reliable networks are vital for information exchange among system components
- Future generation networks will comprise millions of users and connections
- Efficient information propagation affects many networked systems
  - Directing traffic
  - Quarantining patches in networks
  - Regulating spam and rumor spread

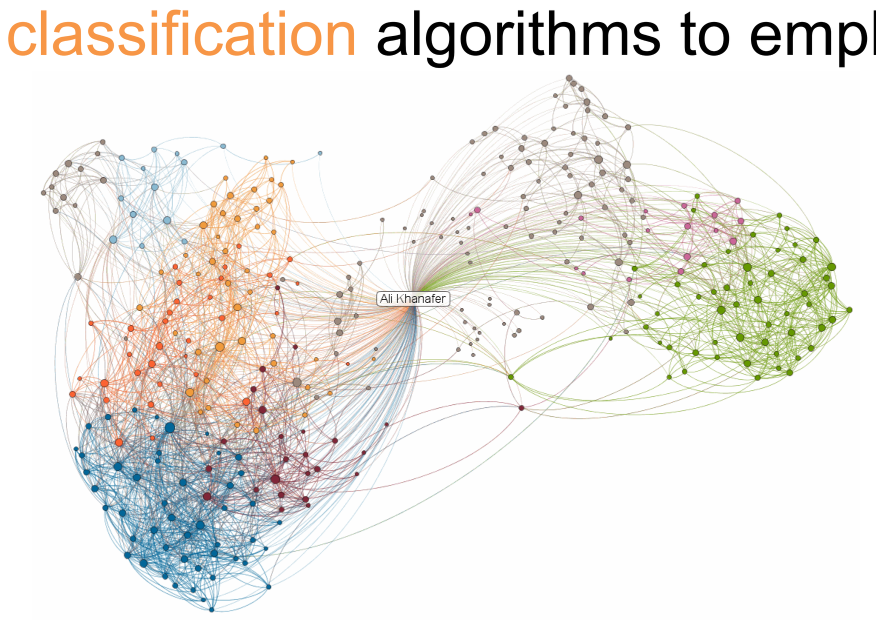


(www.complexification.net)

Goal I: Controllability via Limited Control

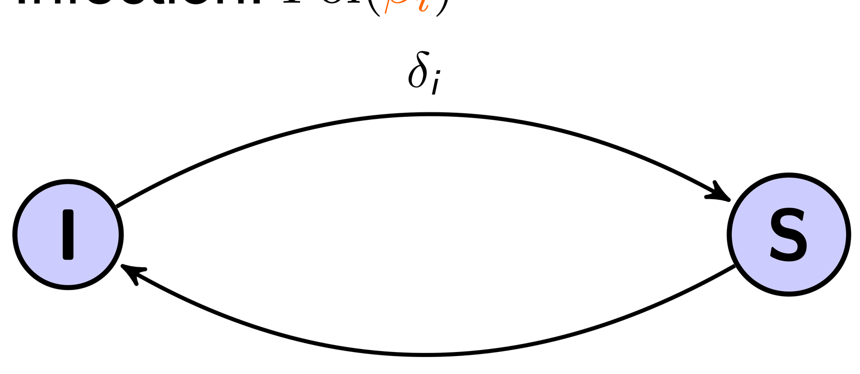
- Information spread control schemes must be scalable
- Common theme: control every node – infeasible and expensive
- Two fundamental questions
  - **Q1:** What is the minimum number of controllers required?
  - **Q2:** Which nodes should be controlled?
- **Approach:** Exploit advances in classification algorithms to employ feedback control theory





Proof of Concept: Virus Spread Control

- Two states per node: healthy or infected
- Curing: $\mathrm{Poi}(\delta_i)$; Infection: $\mathrm{Poi}(\beta_i)$



- Prob. of infection: $p_i(t) \in [0, 1]$. Graph adjacency matrix: A

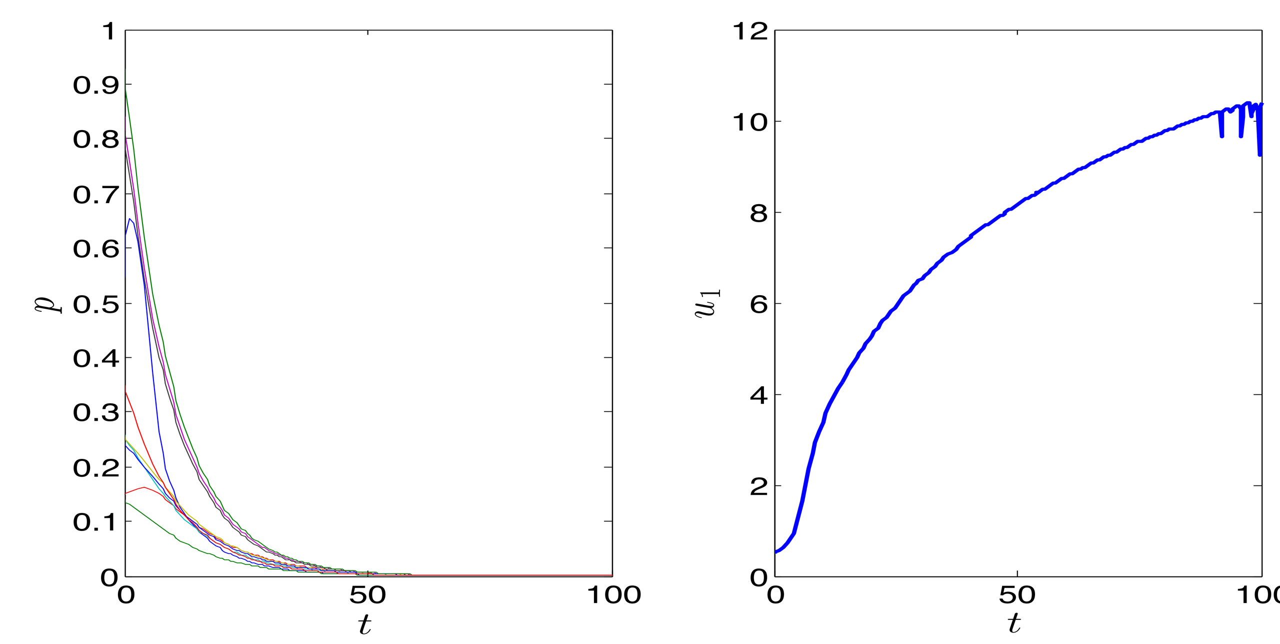
$$\dot{p}(t) = (AB - D - U(t))p(t) - P(t)ABp(t)$$
$$D = \mathrm{diag}(\delta_1, \dots, \delta_n), \quad B = \mathrm{diag}(\beta_1, \dots, \beta_n)$$
$$P = \mathrm{diag}(p_1, \dots, p_n), \quad U = \mathrm{diag}(u_1, \dots, u_n)$$

- Control curing rates of a limited subset of nodes; uncontrolled nodes depend on their arbitrarily small immunity

$$\delta_i = \epsilon \iff u_i = 0$$
$$\delta_i = 0 \iff u_i > 0$$

Low Cost Network Curing

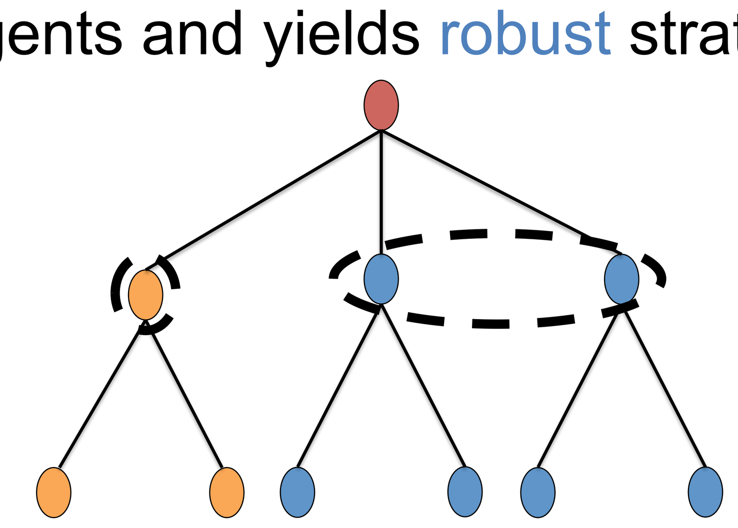
Theorem
Stabilization achieved by placing controls so that no path exists between two uncontrolled nodes



- Implication on required number of control nodes:
  $\text{Star: } 1; \text{ Path: } n/2; \text{ Binary Tree: } \frac{1}{3}(2^\ell - 1), \ell > 2 \text{ (even)}$

Goal II: Robust Distributed Controllers

- Achieve global objectives with limited information about the network
- Objective: implement distributed controllers that are
  - **Feature 1:** Robust to adversarial intervention
  - **Feature 2:** Robust to large modeling uncertainties
- **Approach:** Use a game-theoretic framework which allows for various models of agents and yields robust strategies

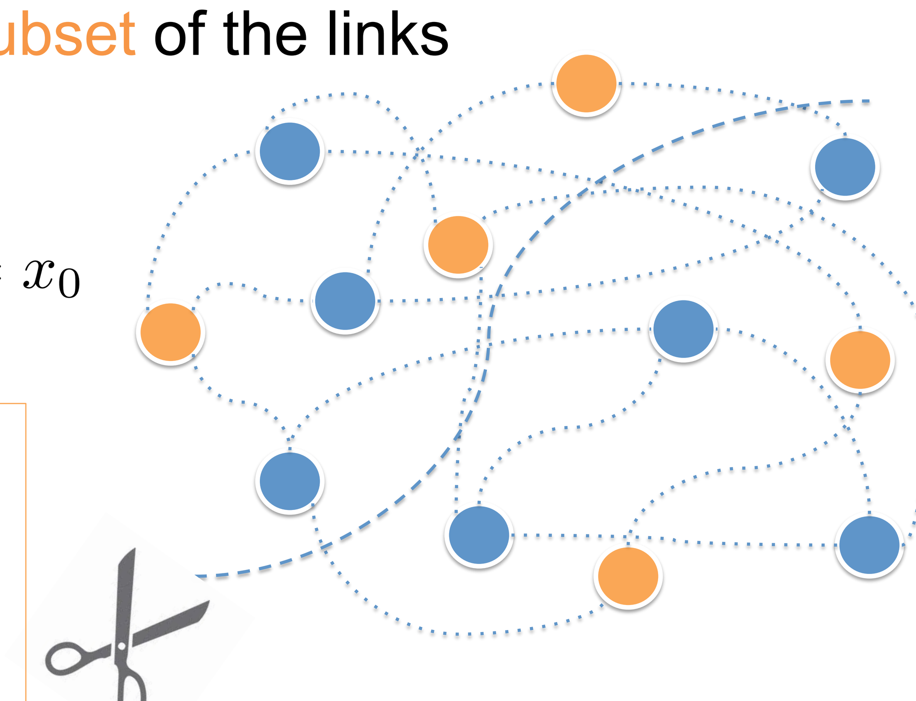


Proof of Concept: Robust Multi-Agent Systems

- Centralized worst-case attack to disrupt distributed computation
- Adversary is allowed to break a subset of the links

$$\max_{u \in \mathcal{U}} \int_0^T k(t)|x - \overline{x}|^2 dt$$
$$\text{subject to} \quad \dot{x} = A(u)x, \quad x(0) = x_0$$
$$||u(t)||_1 \leq \ell$$

Theorem
The optimal strategy at time t is to break ℓ links with maximum $w_{ij}(t) = a_{ij}(x_i(t) - x_j(t))^2$ values



- Implication: Optimal attack depends on local quantities
  - Distributed defense mechanisms can be effective