Networked Cyber-Physical Systems (Net-CPS)

网络 信息-物理 融合 系统

John S. Baras

Institute for Systems Research, University of Maryland, USA
ACCESS Linnaeus Center, Royal Institute of Technology, Sweden
Institute for Advanced Study, Technical University of Munich, Germany

35th CCC
July 27, 2016
Chengdu, China

谢谢**CCC**组委会的邀请

谢谢各位到来

I have been in Chengdu before!

Acknowledgments

- **Joint work with:** Pedram Hovareshti, Tao Jiang, Xiangyang Liu, Peixin Gao, Guodong Shi, George Theodorakopoulos, Shanshan Zheng, Kiran Somasundaram, Ion Matei, Anup Menon
- **Sponsors:** NSF, AFOSR, ARL, ARO, DARPA, NIST, SRC, Lockheed Martin, Northrop Grumman, Telcordia (now ACS), Tage Erlander Guest Profeshorship (KTH), Hans Fischer Senior Fellowship (TUM)

Networked Cyber-Physical Systems

Infrastructure / Communication Networks

Internet / WWW

MANET

Sensor Nets

Robotic Nets

Hybrid Nets: Comm, Sensor, Robotic and Human Nets

Social / Economic Networtks

Social Interactions

Collaboration

Social Filtering

Economic Alliances

Web-based social systems

Biological Networks

Community

Epiddemic

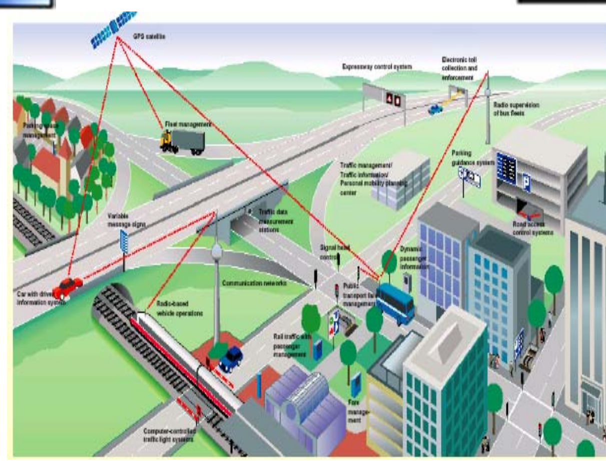
Cellular and Sub-cellular

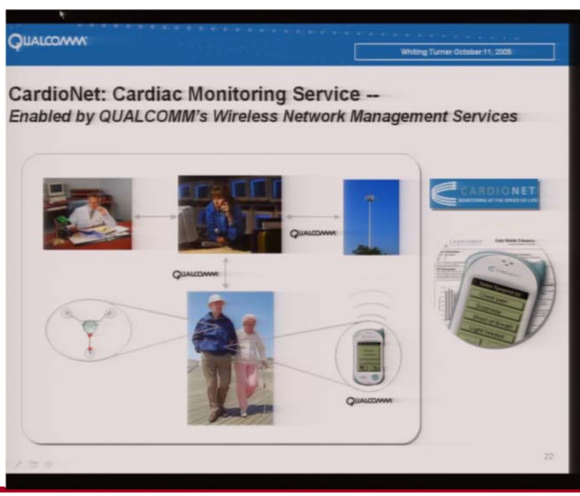
Neural

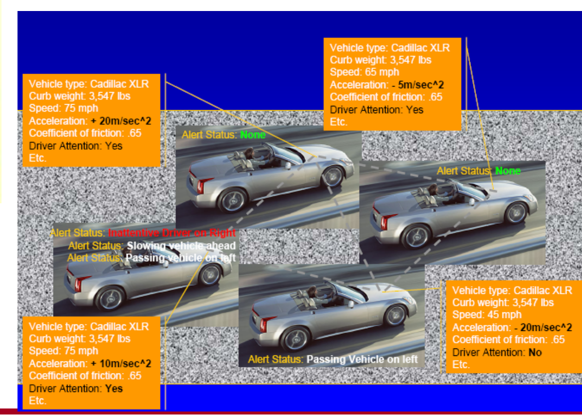
Insects

Animal Flocks

Net-CPS: Wireless and Networked Embedded Systems







iPhone -- Smartphone

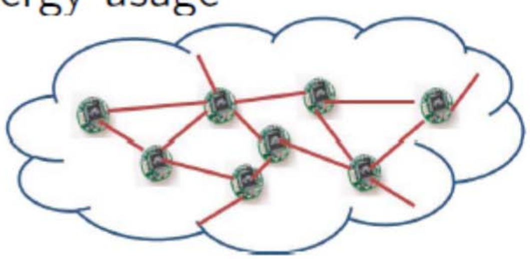
Future “Smart” Homes and Cities

- UI for “Everything”
  - Devices with Computing Capabilities & Interfaces
- Network Communication
  - Devices Connected to Home Network
- Media: Physical to Digital
  - MP3, Netflix, Kindle eBooks, Flickr Photos
- Smart Phones
  - Universal Controller in a Smart Home
- Smart Meters & Grids
  - Demand/Response System for “Power Grid”
- Wireless Medical Devices
  - Portable & Wireless for Real-Time Monitoring

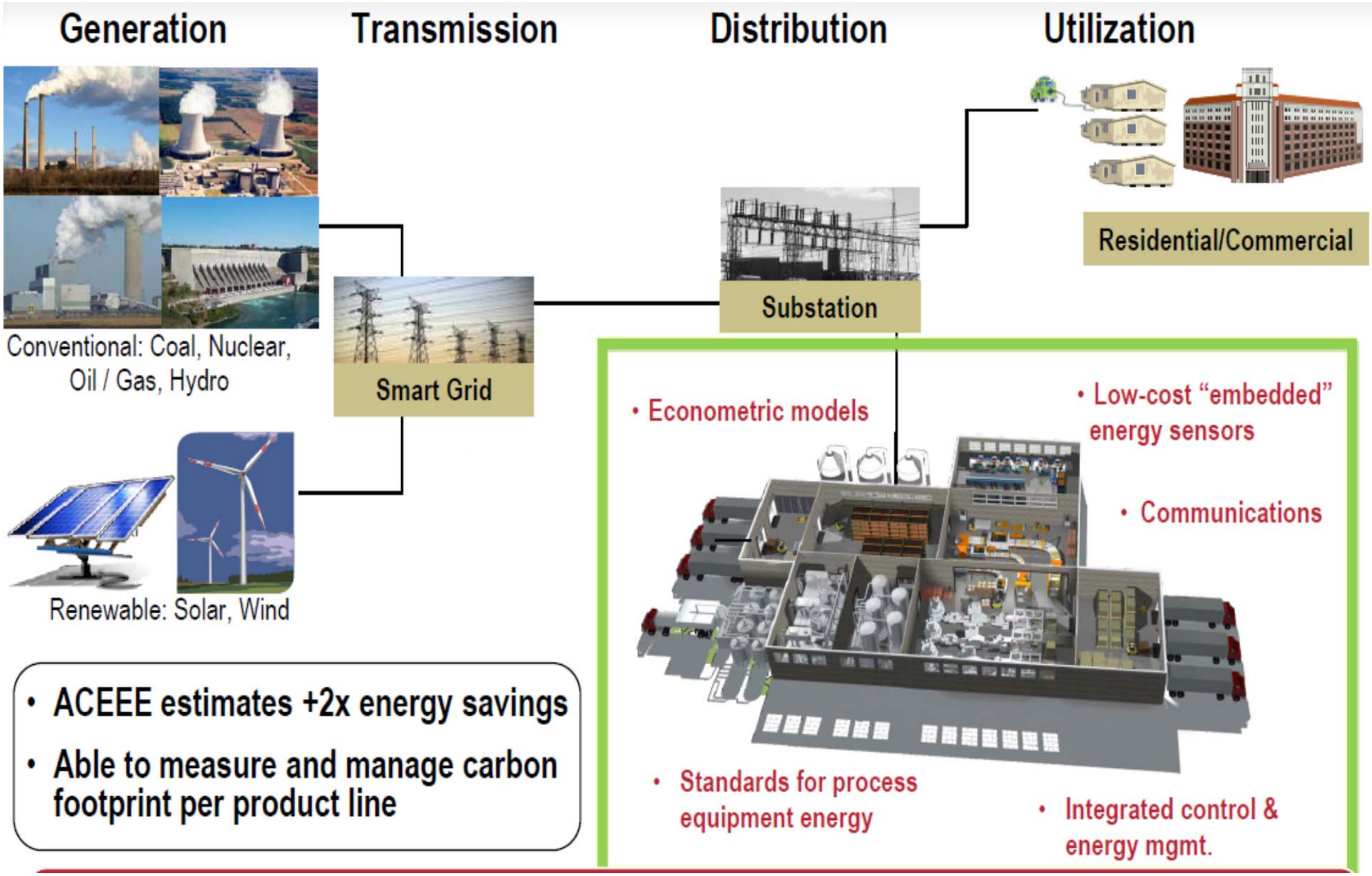

Net-CPS: Wireless Sensor Networks Everywhere

Wireless Sensor Networks (WSN) for infrastructure monitoring

- Environmental systems
- Structural health
- Construction projects
- Energy usage

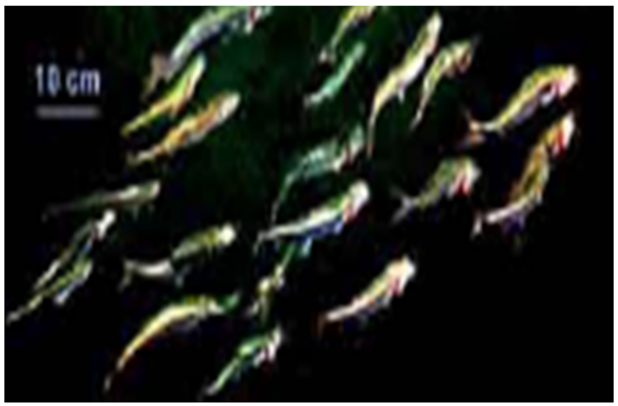


Net-CPS: Smart Grids



- ACEEE estimates +2x energy savings
- Able to measure and manage carbon footprint per product line

Net-CPS: Biological Swarms

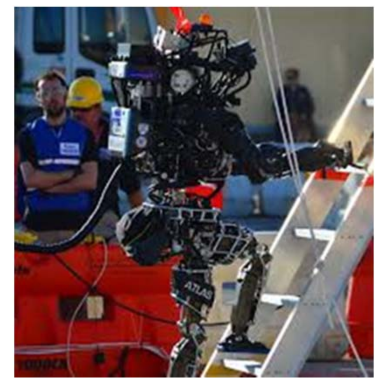


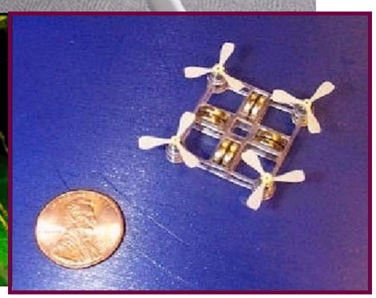
The Institute for Systems Research

Net-CPS:
Collaborative Autonomy

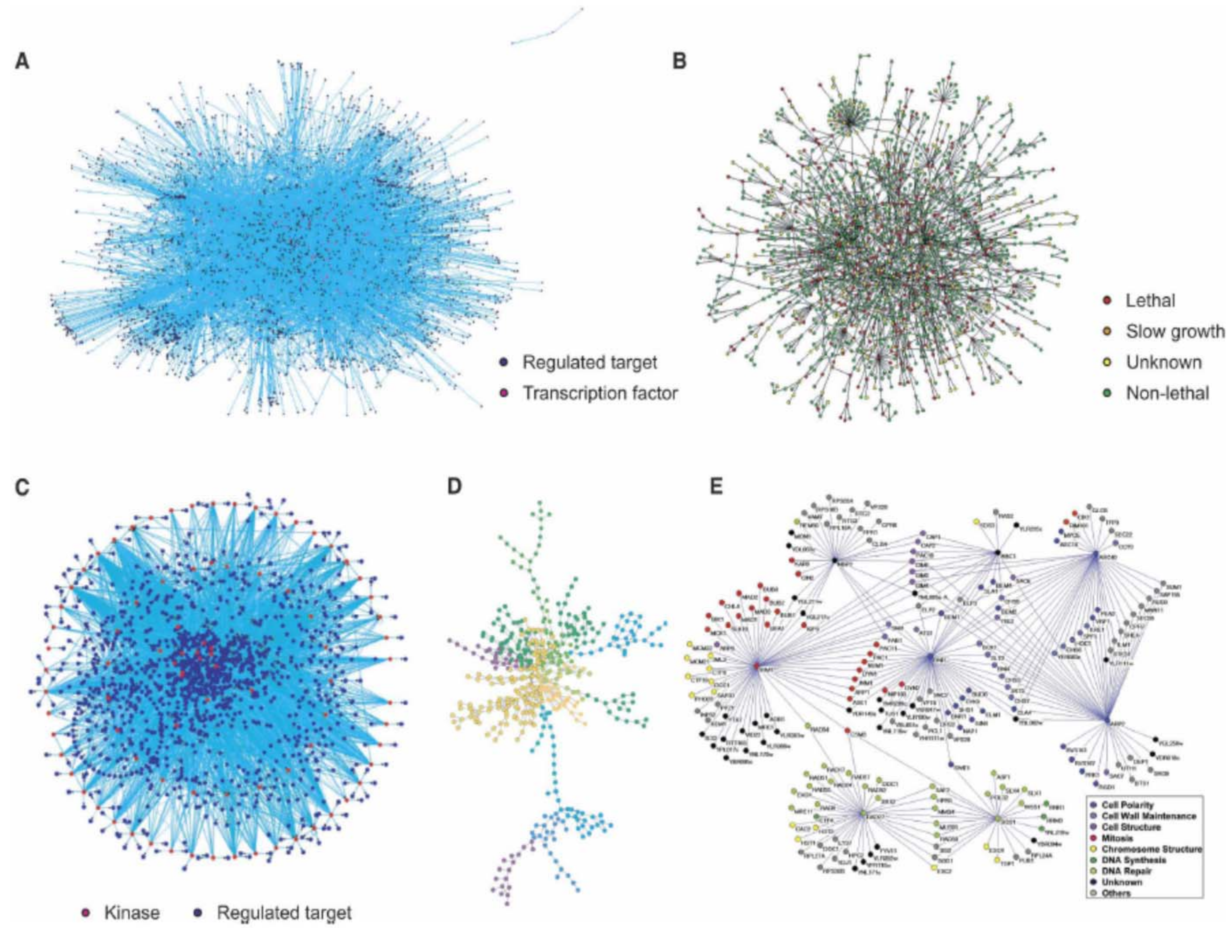
UNIVERSITY OF MARYLAND 1856

- Component-based Architectures
- Communication vs Performance Tradeoffs
- Distributed asynchronous
- Fundamental limits





Net-CPS: Biological Network Types



Examples of biological networks: [A] Yeast transcription factor-binding network; [B] Yeast protein -protein interaction network; [C] Yeast phosphorylation network ; [D] *E. Coli* metabolic network ; [E] Yeast genetic network ; Nodes colored according to their YPD cellular roles [Zhu et al, 2007]

Net-CPS: Social and Economic Networks over the Web

- We are much more “social” than ever before
  - Online social networks (SNS) permeate our lives
  - Such new Life style gives birth to new markets
- Monetize the value of social network
  - Advertising - major source of income for SNS
  - Joining fee, donation etc.
  - …
- Need to know the common features of social networks

CPS and Net-CPS

- **CPS: Technological systems where physical and cyber components are tightly integrated**
- **Examples: smart phones, smart sensors, smart homes, smart cars, smart power grids, smart manufacturing, smart transportation systems, human robotic teams, …**
- **Most of modern CPS are actually networked: via the Internet or the cloud, or via special logical or physical networks**
- **Examples: modern factories, Industrie 4.0, modern enterprises, heterogeneous wireless networks, sensor networks, social networks over the Internet, Industrial Internet (IIC), the Internet of Things (IoT), …**

CPS and Net-CPS

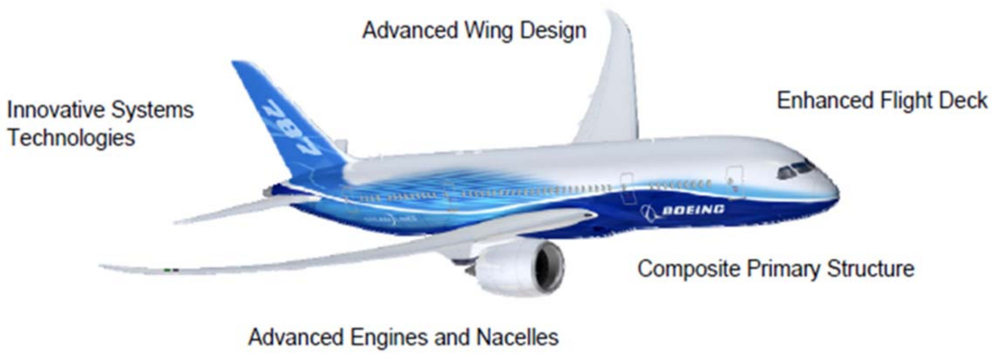
- With networks new fundamental challenges emerge: network semantics and characteristics
- Fundamental challenges on two fronts:
  - (a) on the interface between cyber and physical components and their joint design and performance;
  - (b) on the implications of the networked interfaces and the collaborative aspects of these systems and their design and performance.
- Networked Cyber-Physical Systems (Net-CPS)
- Additional challenge: incorporation of humans in Net-CPS, as system components from start

CPS Architecture: Materials-Geometry-Controls

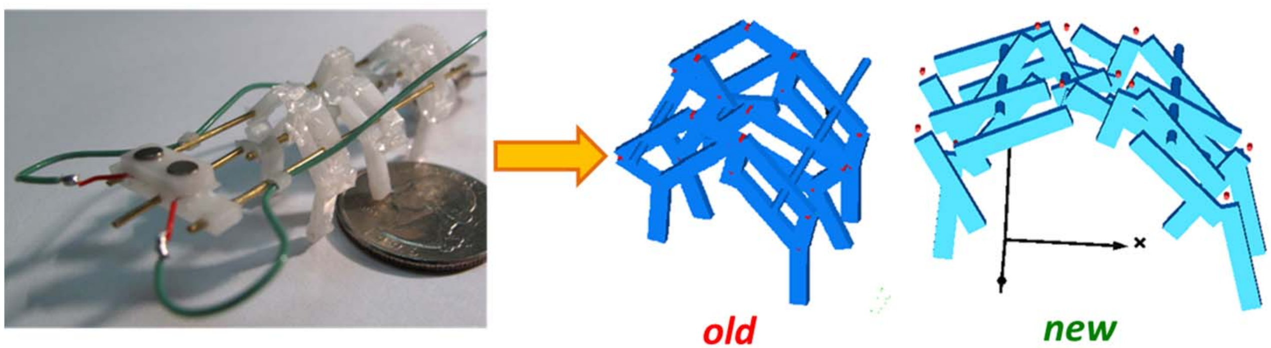
The 787 Dreamliner delivers: *Relative to the 767

- 20%* reduction in fuel and CO_2
- 28% below 2008 industry limits for NOx
- 60%* smaller noise foot print

Composite wing – new control algorithms
All-electric platform – new aircraft VMS



Architecture Logics, their Representation and Integration



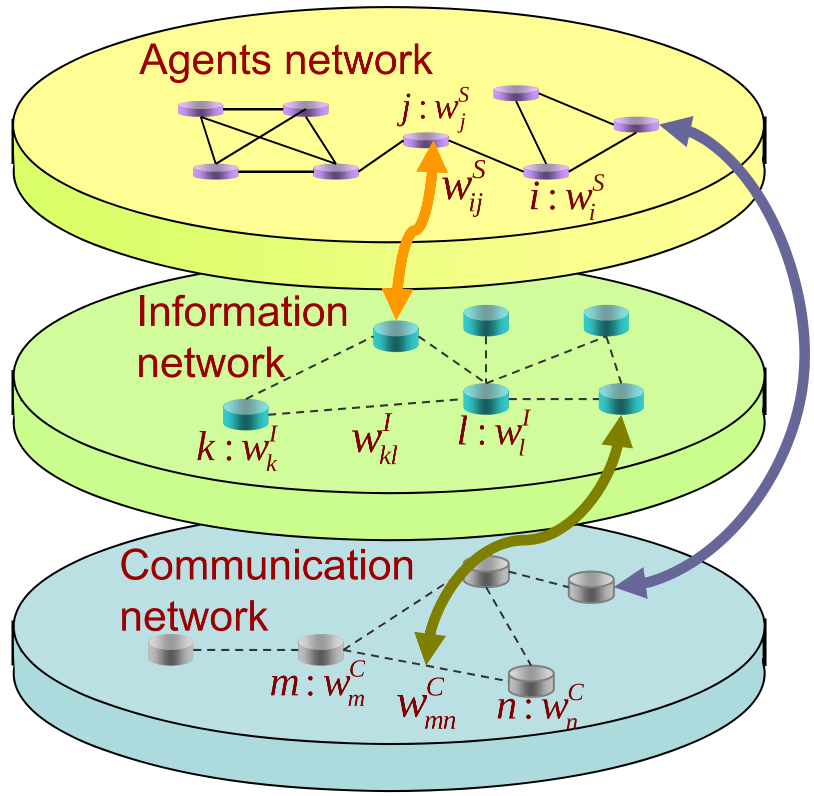
Fast micro-robots – new joint design of geometry-material-controls – More stable and faster running

Outline

- Multiple interacting coevolving multigraphs – three challenges
- Graph Topology Matters
- Networks and Collaboration – Constrained Coalitional Games
- Collaboration, Trust and Mistrust
- New Probabilistic Models
- Conclusions

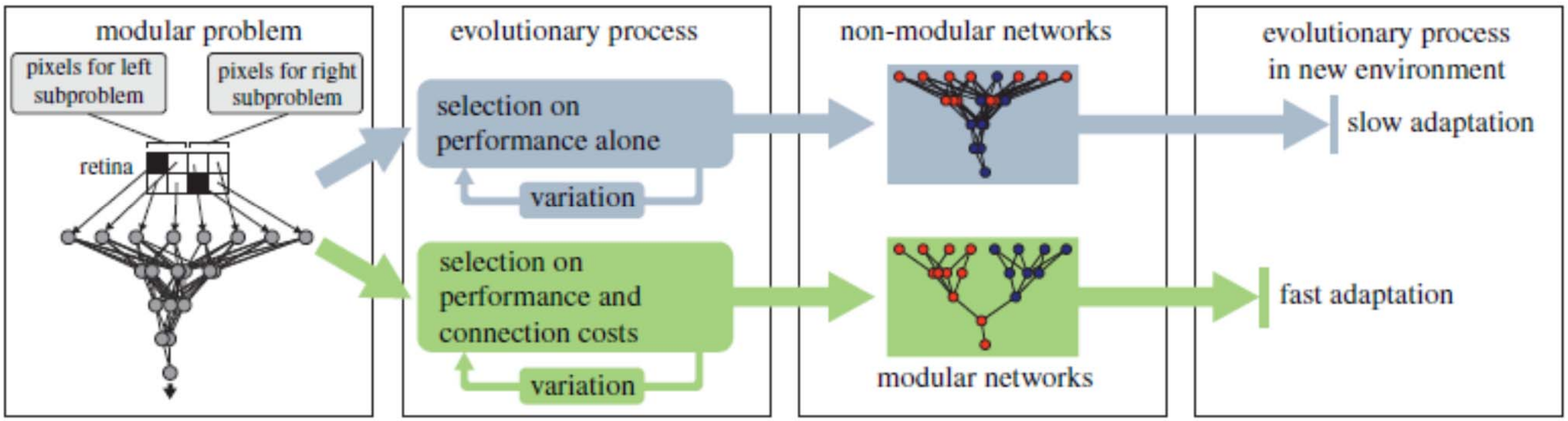
Multiple Coevolving Multigraphs

- Multiple Interacting Graphs
  - *Nodes*: agents, individuals, groups, organizations
  - Directed graphs
  - *Links*: ties, relationships
  - Weights on links : value (strength, significance) of tie
  - Weights on nodes : importance of node (agent)
- **Value directed graphs with weighted nodes**
- **Real-life problems: Dynamic, time varying graphs, relations, weights, policies**



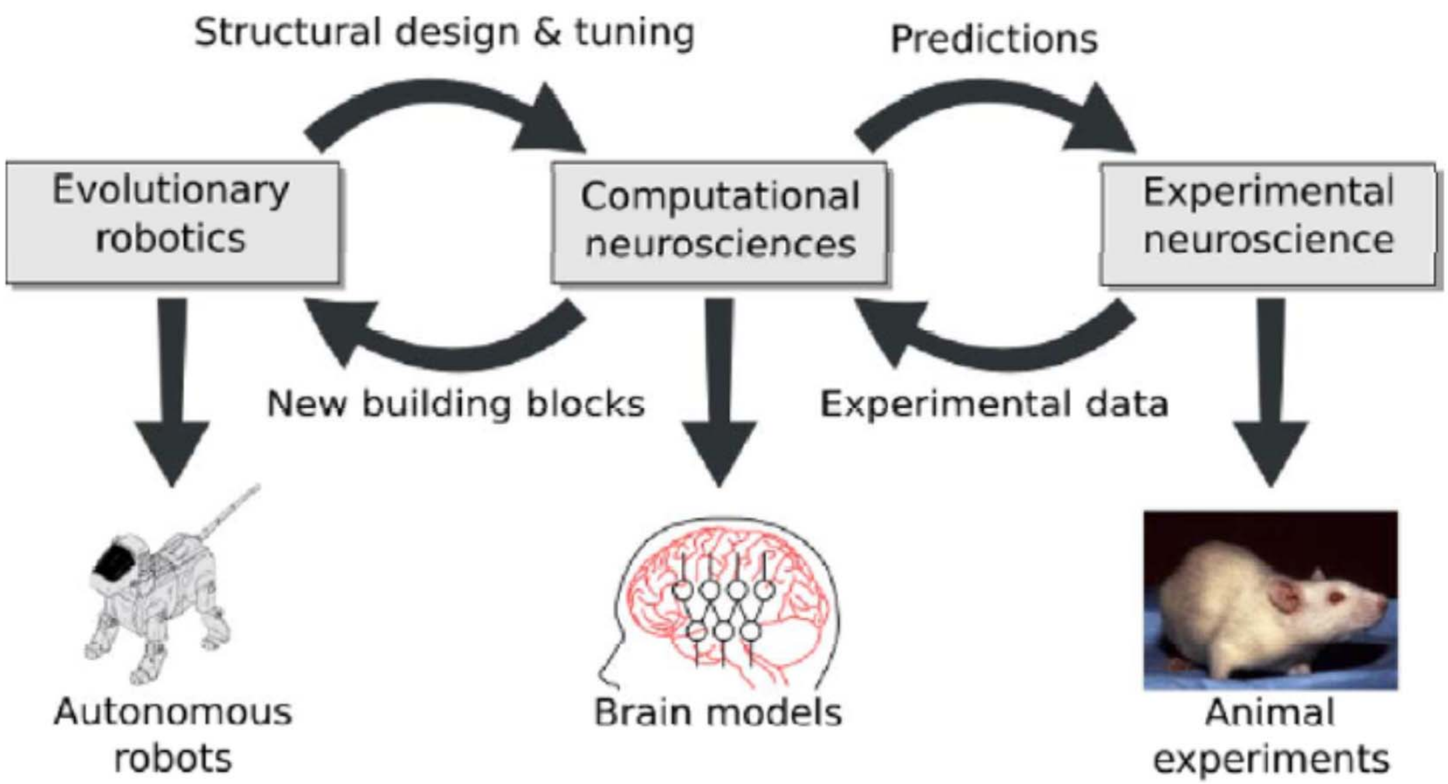
Networked System architecture & operation

Challenges: Modularity vs Performance



- Optimize only on performance – poor adaptivity
- Add cost of communications – improved adaptivity
- Communication motifs
- Evolvable modularity for some networked CPS?

Neural Network Evolution:
from programmed structure to function feedback on structure



Three Fundamental Challenges

- **Multiple interacting coevolving multigraphs involved**
  - ***Collaboration multigraph***: who has to collaborate with whom and when.
  - ***Communication multigraph***: who has to communicate with whom and when
- **Effects of connectivity topologies**:
  Find graph topologies with favorable tradeoff between performance improvement (**benefit**) of collaborative behaviors *vs* **cost** of collaboration
  - **Small word graphs** achieve such **tradeoff**
  - **Two level algorithm** to provide efficient communication
- Need for **different probability models** – the classical Kolmogorov model is **not correct**
  - Probability models over logics and timed structures
  - Logic of projections in Hilbert spaces – not the Boolean of subsets

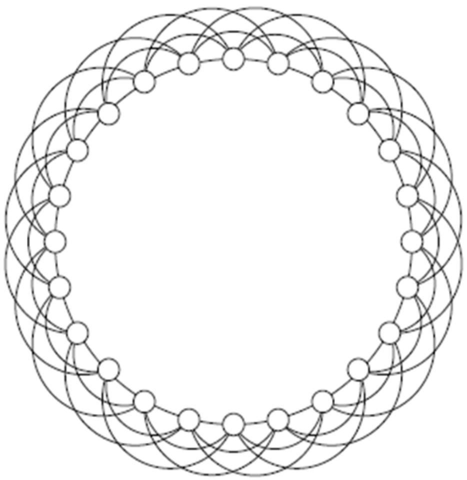
Distributed Algorithms in Networked Systems and Topologies

- Distributed algorithms are essential
  - Agents **communicate with neighbors,** share/process information
  - Agents **perform local** actions
  - **Emergence** of global behaviors
- **Effectiveness** of distributed algorithms
  - The **speed** of convergence
  - **Robustness** to agent/connection failures
  - Energy/ communication **efficiency**
- **Design problem**:

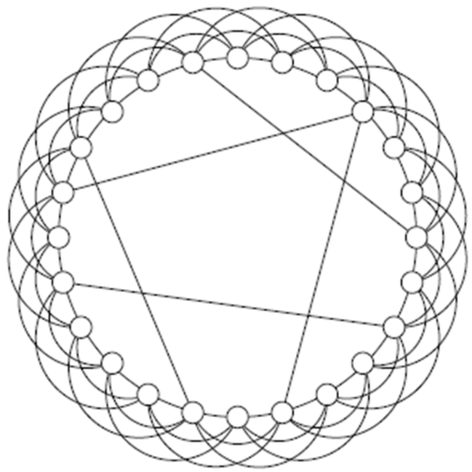
  Find graph topologies with favorable tradeoff between performance improvement (**benefit**) *vs* **cost** of collaboration
- **Example: Small Word graphs** in consensus problems

An Example problem of the Interaction between the Control Graph and the Communication Graph

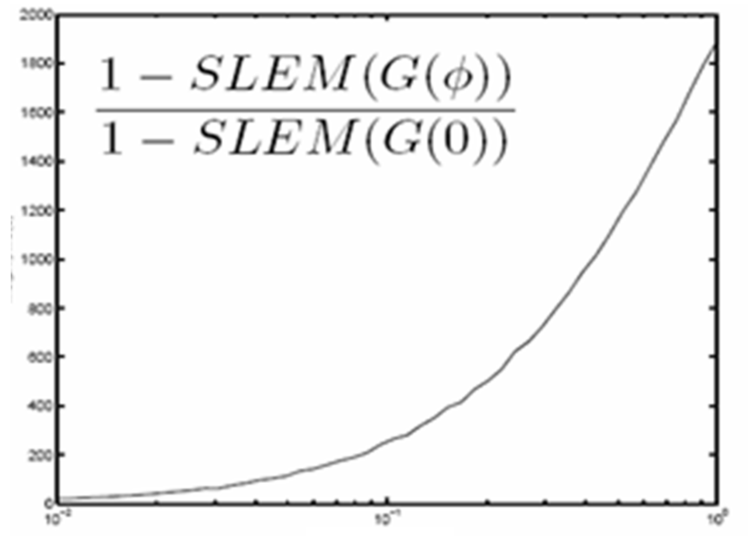
Small World Graphs



Simple Lattice
C(n,k)



Small world: Slight variation adding $nk\Phi$



\phi
C(1000,5)

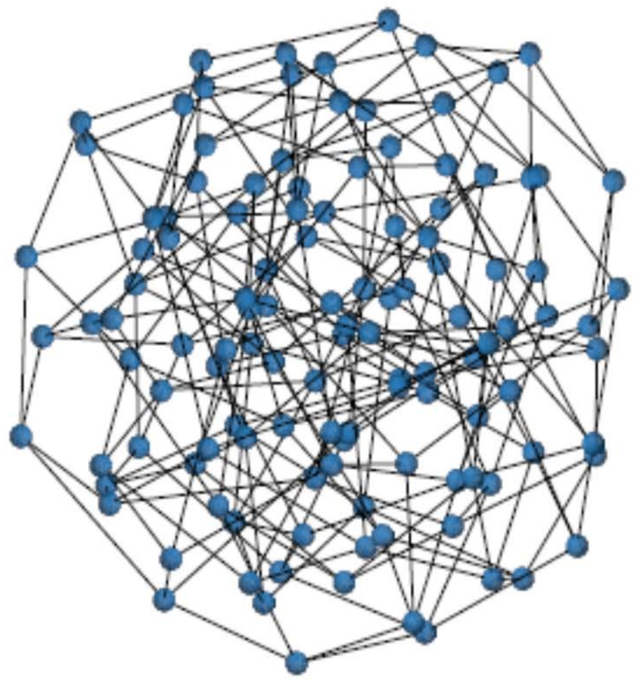
Adding a **small portion** of well-chosen links → **significant increase** in convergence rate

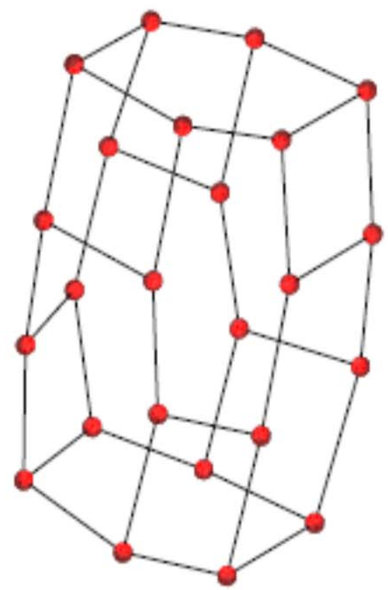
Expander Graphs

- First defined by Bassalygo and Pinsker -- 1973
- Fast synchronization of a network of oscillators
- Network where any node is "nearby" any other
- Fast 'diffusion' of information in a network
- Fast convergence of consensus
- Decide connectivity with smallest memory
- Random walks converge rapidly
- Easy to construct, even in a distributed way (ZigZag graph product)
- Graph G, ***Cheeger constant h(G)***
  - All partitions of G to S and S^c,

    $h(G)$=min (#edges connecting S and S^c) / (#nodes in smallest of S and S^c)
- (k, N, ε) **expander** : $h(G) > \varepsilon$; **sparse but locally well connected** **(1-*SLEM*(G) increases as $h(G)^2$)**

Expander Graphs – Ramanujan Graphs

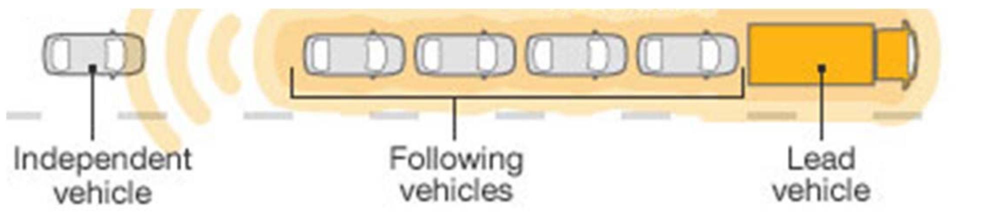




An Example: Vehicle Platooning

Consider an Intelligent Vehicle Highway System (IVHS) where a number of vehicles heading to a common destination form a platoon or a road train.
Advantages-

- improved highway throughput and
- reduced fuel consumption.



High Speeds, Close Spacing and Multiple Vehicles
➔Need Automatic Distributed Control

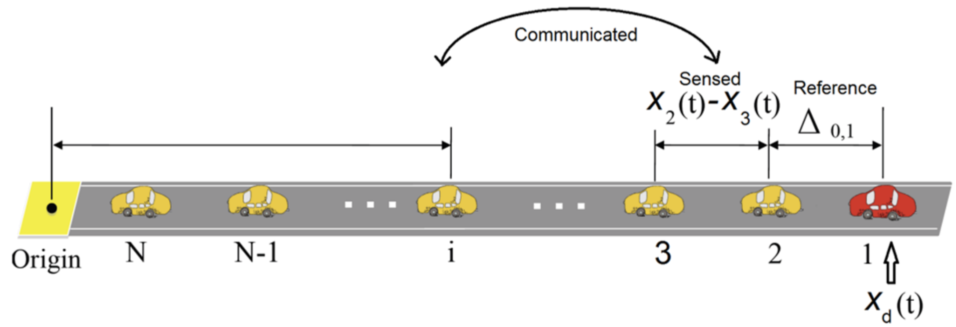
Brief Literature Review

- Vehicles have identical linear dynamics

$$\ddot{x}_i = u_i.$$

- Only lead vehicle is given desired trajectory information $x_d(t)$.
- Symmetric Control: *i* applies a linear feedback law based information available

$$u_i = \frac{1}{deg(i)} \sum_{j \in \mathcal{N}(i)} [-k(x_i - x_j - \Delta_{i,j}) - b(\dot{x}_i - \dot{x}_j)] + \delta(1,i)[-k(x_1 - x_{1,d}) - b(\dot{x}_1 - \dot{x}_{1,d})]$$



Control objective:
Regulation- maintain prescribed reference inter-vehicle spacing.

If the information is restricted to the nearest neighbor type, then

- The least damped eigenvalue of the closed loop matrix scales as $O(1/N^2)$
- String instability is inevitable- disturbances acting on an individual grow without bounds in the size of the platoon.
- It is not possible to achieve coherence or resemblance to a rigid lattice as the formation moves.

Bottom line:
Nearest neighbor type information patterns lead to inadequate control performance.

Vehicle Platooning Problem: Better Information Pattern

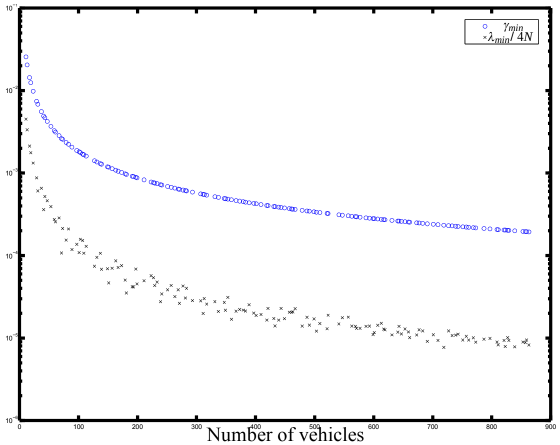
Information pattern	Communication load ~ |Edges|	Stability margin
Nearest neighbor type	O(N)	$O(1/N^2)$
Complete graph	$O(N^2)$	At most O(1/N)

- Is there something in between? Does there exist a “family” of graphs such that one can get improved control performance while limiting the communication load?

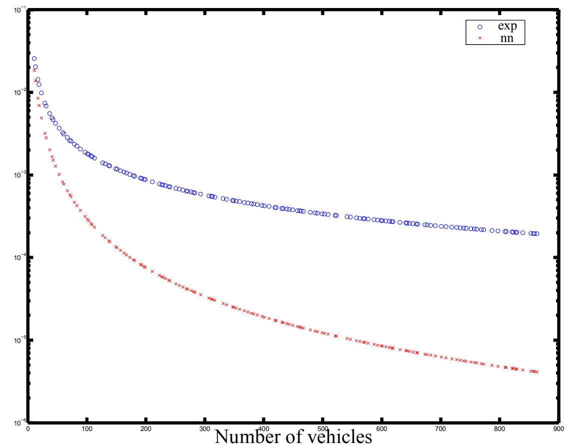
- Our result (Menon-Baras 2012-2013):

Expander families	O(N)	At most O(1/N)

Some Numerical Simulations and Next Steps



➢ An experimental verification of the main result stated earlier. The plot of the stability margin γ_{min} is above the lower bound $\frac{\lambda_{min}}{4N}$.



➢ Experimental verification that expanders outperform nearest neighbor type information patterns. Plot of stability margins with expanders serving as information pattern is above that with nearest neighbor type.

Next steps-

➢ Investigate the problem under other metrics of control performance like string stability, coherence etc.

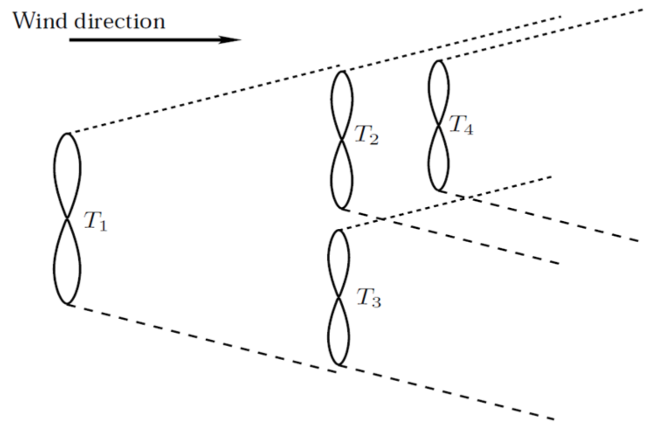
➢ How to synthesize the right expander family?

➢ More general scenarios for answering the question ***"the right information pattern for a given collaborative control task"*.**

Interaction Between Control and Communication Graphs: Agents Learn What is Best for the Team

Example: Maximizing Power Production of a Wind Farm

Horns Rev 1. Photographer Christian Steiness



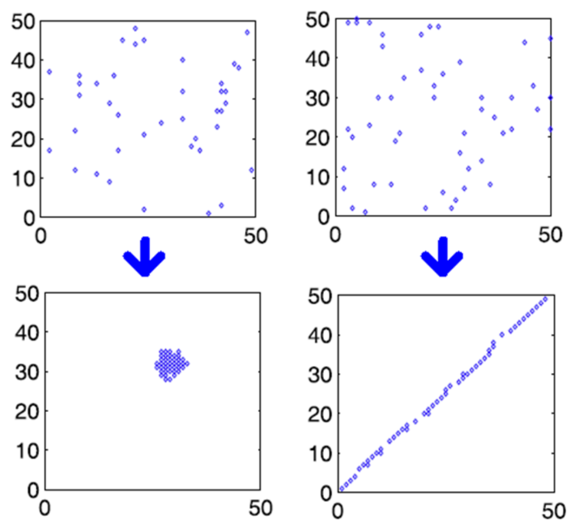
Schematic representation of a wind farm depicting individual turbine wake regions.

- Aerodynamic interaction between different turbines is not well understood.
- Need on-line decentralized optimization algorithms to maximize total power production.

Assign individual utility
$u_i(t) =$ power produced by turbine *i* at time *t*
such that maximizing $\sum_i u_i(t)$ leads to desirable behavior.

Interaction Between Control and Communication Graphs

Example: Formation Control of Robotic Swarms



Simulation results demonstrating rendezvous and gathering along a line[2]

- Deploy a robotic swarm in unknown environment: obstacles, targets etc. have to be discovered.[3]
- The swarm must form a prescribed geometric formation.
- Robots have limited sensing and communication capabilities.

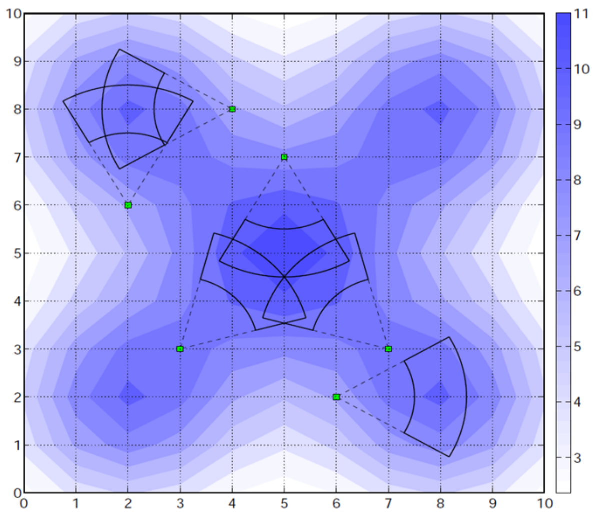
For rendezvous, design individual utility

$$u_i(s_i) = \frac{1}{|\{s_j \in S: \|s_i - s_j\| < r\}|} - \alpha \, dist_r(s_i, obstacle),$$

such that minimizing $\sum_i u_i(t)$ leads to desirable behavior.

Interacting Control, Information and Communication Graphs

Example: Mobile Visual Sensor Network Deployment



Darker the shade of blue, more the interest in the site. Sectors represent sensor position and camera viewing angle.

- We wish to monitor events in different sites of varying interest levels.
- All robots monitoring a small set of high interest sites is undesirable w.r.t. coverage.
- Cost associated with information processing.
- How to deploy so “effective coverage" is ensured at “reasonable cost".

Design individual utility

$$u_i(s, c) = \sum_{s' \in NB(s,c)} \frac{q(s')}{n(s')} - f_i(c),$$

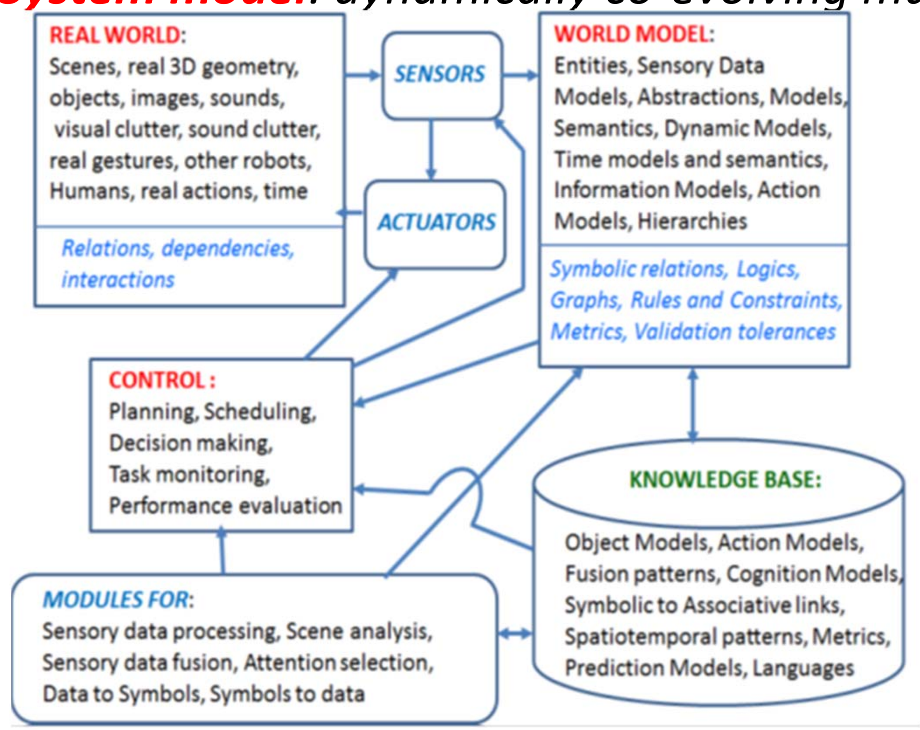
such that maximizing $\sum_i u_i(t)$ leads to desirable behavior.

(here q(s)= interest in observing s, n(s) = number of agents observing s, NB(s,c) = subset of S observable from s when camera viewing angle= c, and $f_i(c)$ = processing cost when the camera viewing angle is c.)

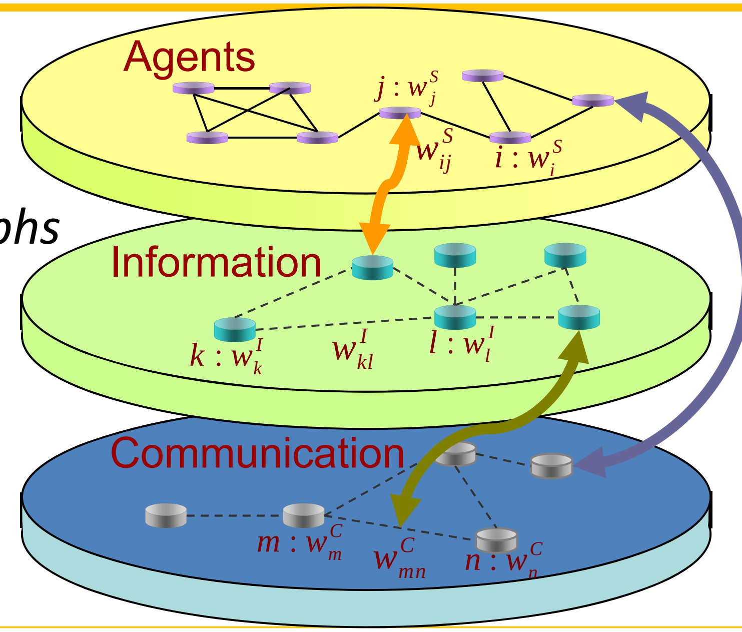
Net-CPS and Collaborative Autonomy

Collaborating agents architecture

- *Nodes and links annotated by weights or rules*
- *Annotations are associated across layers,*
- ***System model**: dynamically co-evolving multigraphs*



Each node carries this real vs world model framework



Task-driven integration of perception, control, language

- *Cognitive dialogue*
- *Dynamic attention mechanism*
- *Manipulation grammar*
- *Three-layer architecture*

A Network is …

- A collection of nodes, agents, …

  that **collaborate** to accomplish actions, gains, …

  that cannot be accomplished with out such collaboration

- Most significant concept for **dynamic autonomic networks**

The Fundamental Trade-off

- The nodes **gain** from collaborating
- But collaboration has **costs** (e.g. **communications)**
- **Trade-off: gain from collaboration *vs* cost of collaboration**

  Vector metrics involved typically

  → **Constrained Coalitional Games**

- **Example 1**: **Network Formation** -- Effects on Topology
- **Example 2**: **Collaborative robotics, communications**
- **Example 3**: **Web-based social networks and services**
- **Example 4**: **Groups of cancer tumor or virus cells**

• • •

Gain

- Users gain by joining a coalition.
  - **Wireless networks**
    - The benefit of nodes in wireless networks can be the rate of data flow they receive, which is a function of the received power

$$B_{ij} = f(P_j l(d_{ij}))$$

P_j is the power to generate the transmission and $l(d_{ij}) < 1$ is the loss factor

e.g: $B_{ij} = \log(1 + (P_j l(d_{ij}) / N_0))$

  - **Social connection** model (Jackson & Wolinsky 1996)

$$B_{ij} = \sum_{j \in g} V \delta^{r_{ij} - 1} \quad \text{or} \quad w_i(G)$$

    - r_{ij} is # of hops in the shortest path between i and j
    - $0 \le \delta \le 1$ *is the connection gain depreciation rate*

Cost

- Activating links is costly. $c_i(G) = \sum_{j \in N_i^t} C_{ij}$
  - **Wireless networks**
    - Energy consumption for sending data: $C_{ij} = RSd_{ij}^{\alpha}$

      RS depends on transmitter/receiver antenna gains and system loss not related to propagation

      α : path loss exponent
    - Data loss during transmission

      v_i is the environment noise and I_{ij} is the interference

      $$C_{ij} = h(v_i, I_{ij}) > 0$$
  - **Social connection model**
    - The more a node is **trusted**, the lower the cost to establish link

      e.g.suppose that the trust i has on j is s_{ij} (between 0 and 1), we can define the cost as the inverse of the trust values

      $$C_{ij} = 1 / s_{ij}$$

Pairwise Game and Convergence

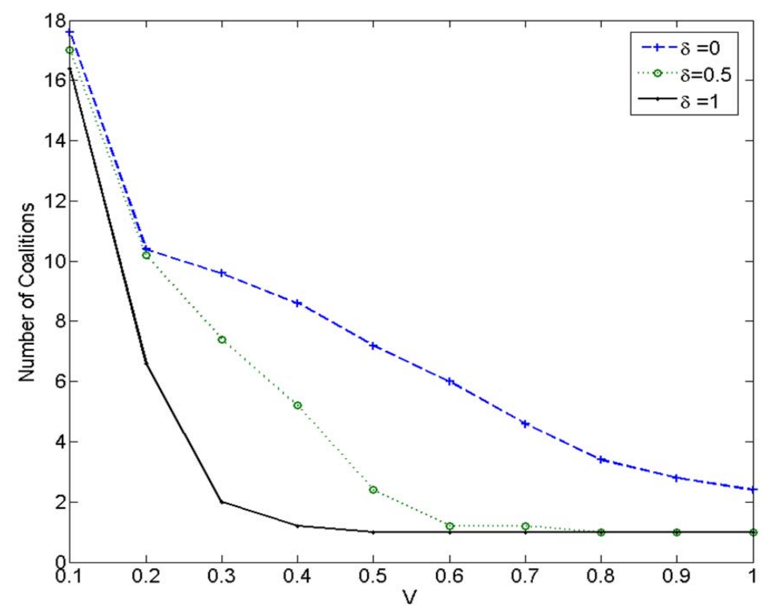
- Payoff of node $\boldsymbol{i}$ from the network G is defined as

$$v_i(G) = \text{gain} - \text{cost} = w_i(G) - c_i(G)$$

- Iterated process
  - Node pair $\boldsymbol{ij}$ is selected with probability $\boldsymbol{p_{ij}}$
  - If link $\boldsymbol{ij}$ is already in the network, the decision is whether to sever it, and otherwise the decision is whether to activate the link
  - The nodes act myopically, activating the link if it makes each at least as well off and one strictly better off, and deleting the link if it makes either player better off
  - **End**: if after some time, no additional links are formed or severed
  - **With random mutations** , the game converges to a unique Pareto equilibrium (underlying Markov chain states)

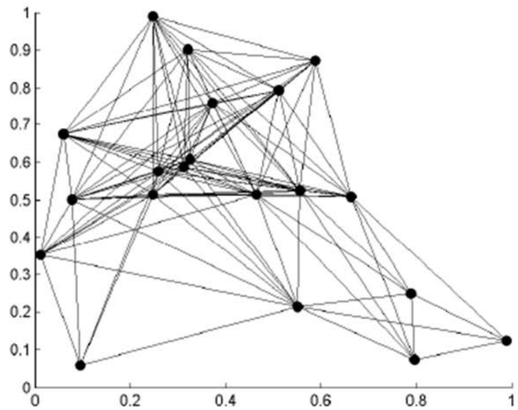
Coalition Formation at the Stable State

- The cost depends on the physical locations of nodes
  - Random network where nodes are placed according to a uniform Poisson point process on the [0,1] x [0,1] square.
- Theorem: The coalition formation at the stable state for n→∞
  - Given $\delta = 0, \quad V = P\left(\frac{\ln n}{n}\right)^{\frac{\alpha}{2}}$ is a sharp threshold for establishing the grand coalition (number of coalitions = 1).
  - For $0 < \delta \leq 1$, the threshold is less than $P\left(\frac{\ln n}{n}\right)^{\frac{\alpha}{2}}$.

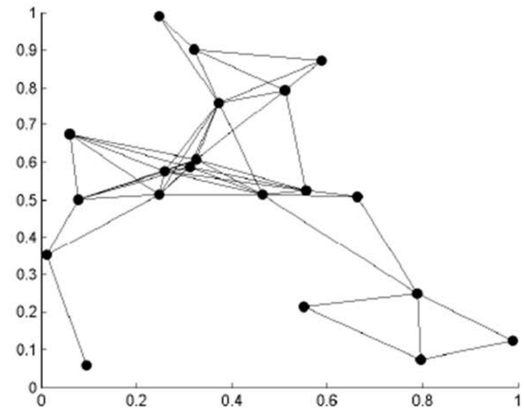


n = 20

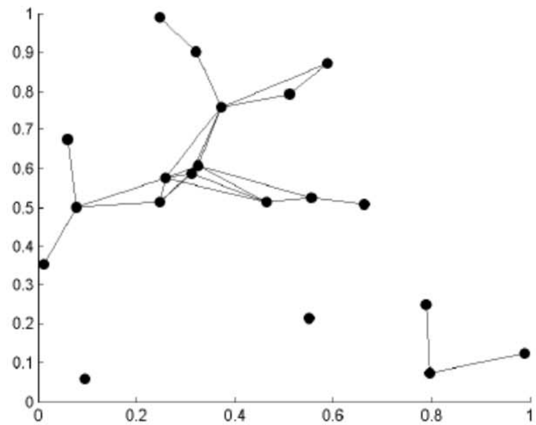
Topologies Formed



(a) P = 0.5 (low cost); complete graph



(b) P = 2 (middle cost); small world topology



(c) P = 4 (high cost); partitioned network

Trust as Mechanism to Induce Collaboration

- Trust **is an incentive** for collaboration (Arrow 1974)
  - Nodes who refrain from cooperation get lower trust values
  - Eventually penalized because **other nodes tend to only cooperate with highly trusted ones**.
- For node i **loss for not cooperating** with node j is a nondecreasing function of J_{ji}, $f(J_{ji})$,
- New characteristic function is

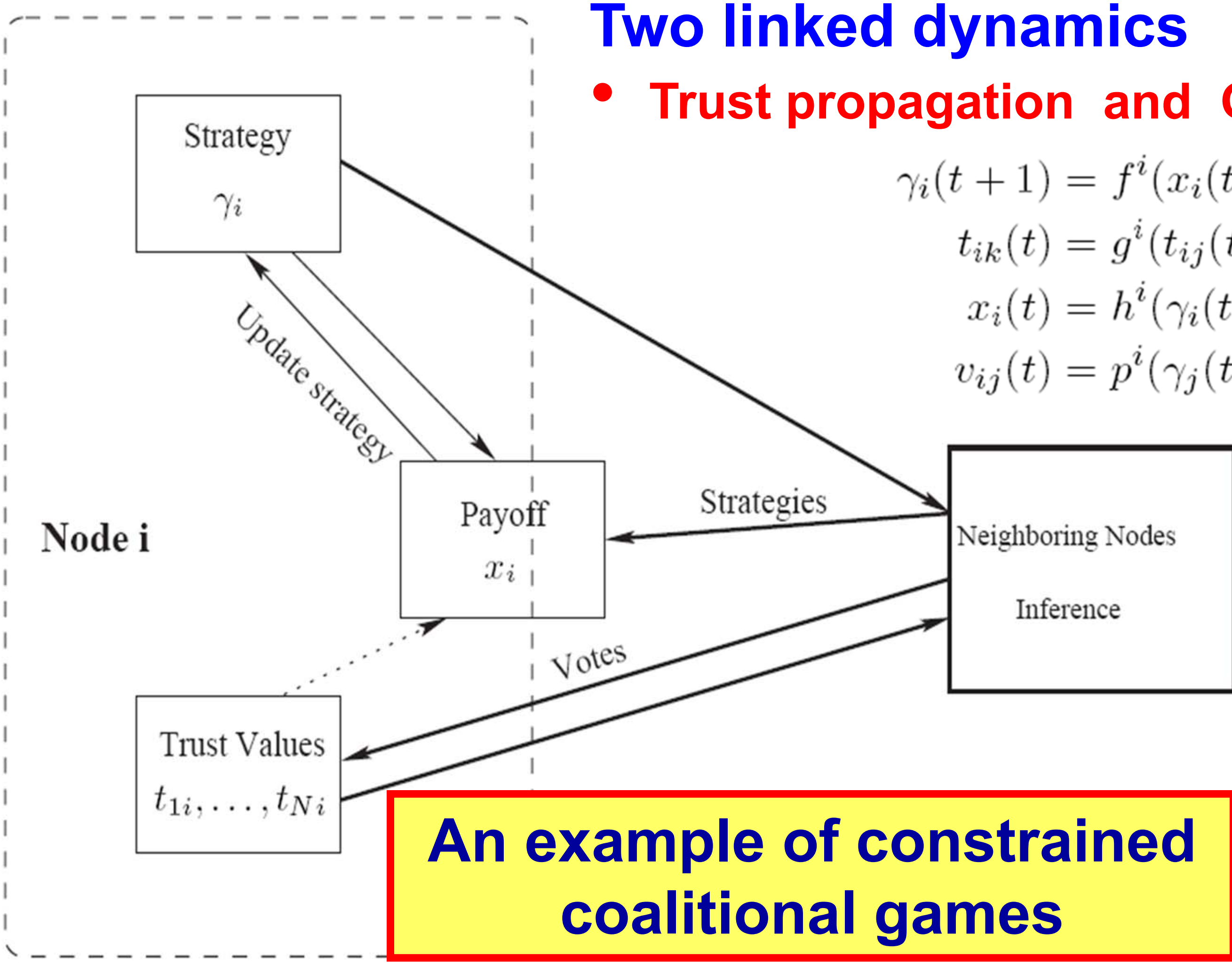
$$\nu(\mathcal{S}) = \sum_{i,j \in \mathcal{S}} J_{ij} - \sum_{i \in \mathcal{S}, j \notin \mathcal{S}} f(J_{ij})$$

(*Baras-Jiang 04, 05*)

- **Theorem**: if $\forall i, j, J_{ij} + f(J_{ji}) \geq 0$, the core is nonempty and $x_i = \sum_{j \in N_i} J_{ij}$ is a feasible payoff allocation in the core.

By introducing a trust mechanism, all nodes are induced to collaborate without any negotiation

Dynamic Coalition Formation



Two linked dynamics

- **Trust propagation and Game evolution**

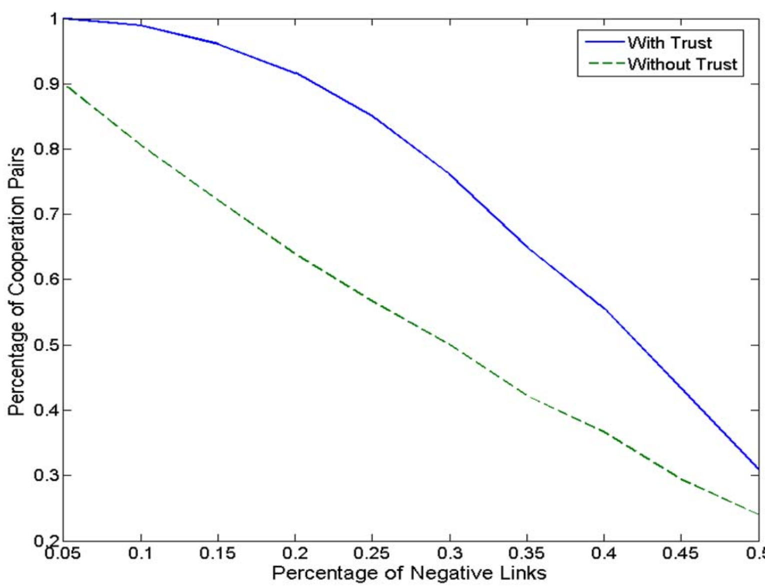
$$\gamma_i(t+1) = f^i(x_i(t), \gamma_i(t), \gamma_j(t), t_{ij}(t))$$
$$t_{ik}(t) = g^i(t_{ij}(t), v_{jk}(t)) \quad \forall k \in N$$
$$x_i(t) = h^i(\gamma_i(t), \gamma_j(t))$$
$$v_{ij}(t) = p^i(\gamma_j(t), t_{ji}(t))$$

An example of constrained coalitional games

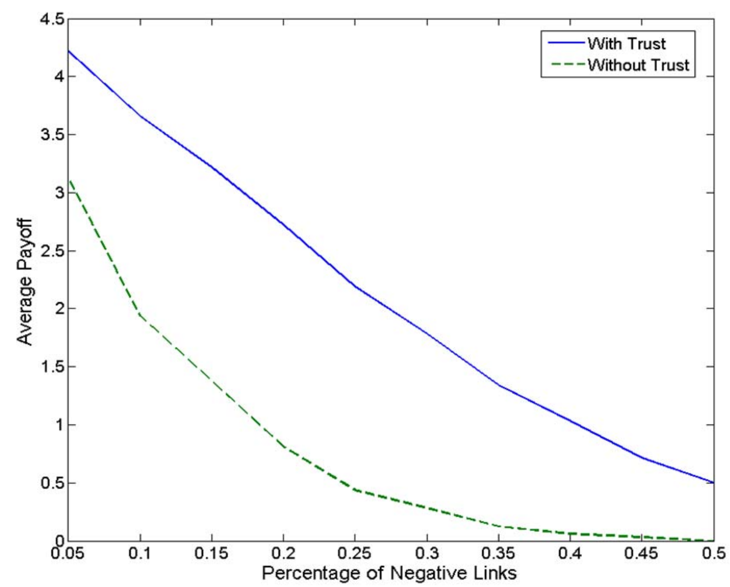
Stability of dynamic coalition Nash equilibrium

Results of Game Evolution

- **Theorem**: $\forall i \in N_i$ and $x_i = \sum_{j \in N_i} J_{ij}$, there exists τ_0, such that for a reestablishing period $\tau > \tau_0$ *(Baras-Jiang 05, 09, 10)*
  - terated game converges to Nash equilibrium;
  - In the Nash equilibrium, all nodes cooperate with all their neighbors.
- Compare games with (without) trust mechanism, strategy update:



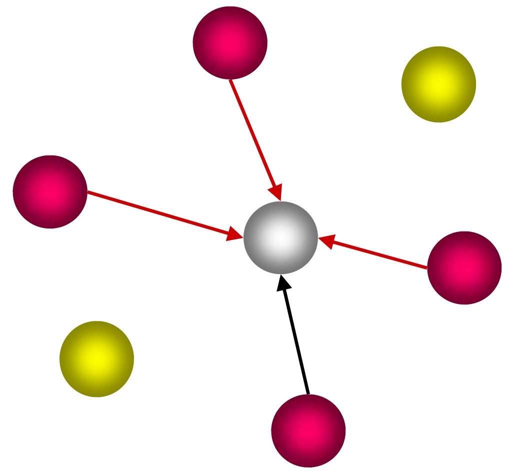
Percentage of cooperating pairs *vs* negative links



Average payoffs *vs* negative links

Trust Evaluation: Local Voting Rule

- In homogenous networks, the trustworthiness of an agent is based on other peers' opinion
  - The most straightforward scheme is to ask neighbors to "vote" for it
  - Values of the votes are equal to c_{ij}



- Iterative voting rule:

$$s_i(k+1) = f\left(J_{ji} s_j(k) \mid j \in N_i\right)$$

  - Evaluation starts from a small set of trusted nodes
  - Our interest is to study evolution of the estimated trust value s_i and its property at the equilibrium

More Generally: Node Dynamics

$$x_i(k+1) = f_i\Big(x_i(k); x_j(k), j \in \mathcal{N}_i\Big)$$

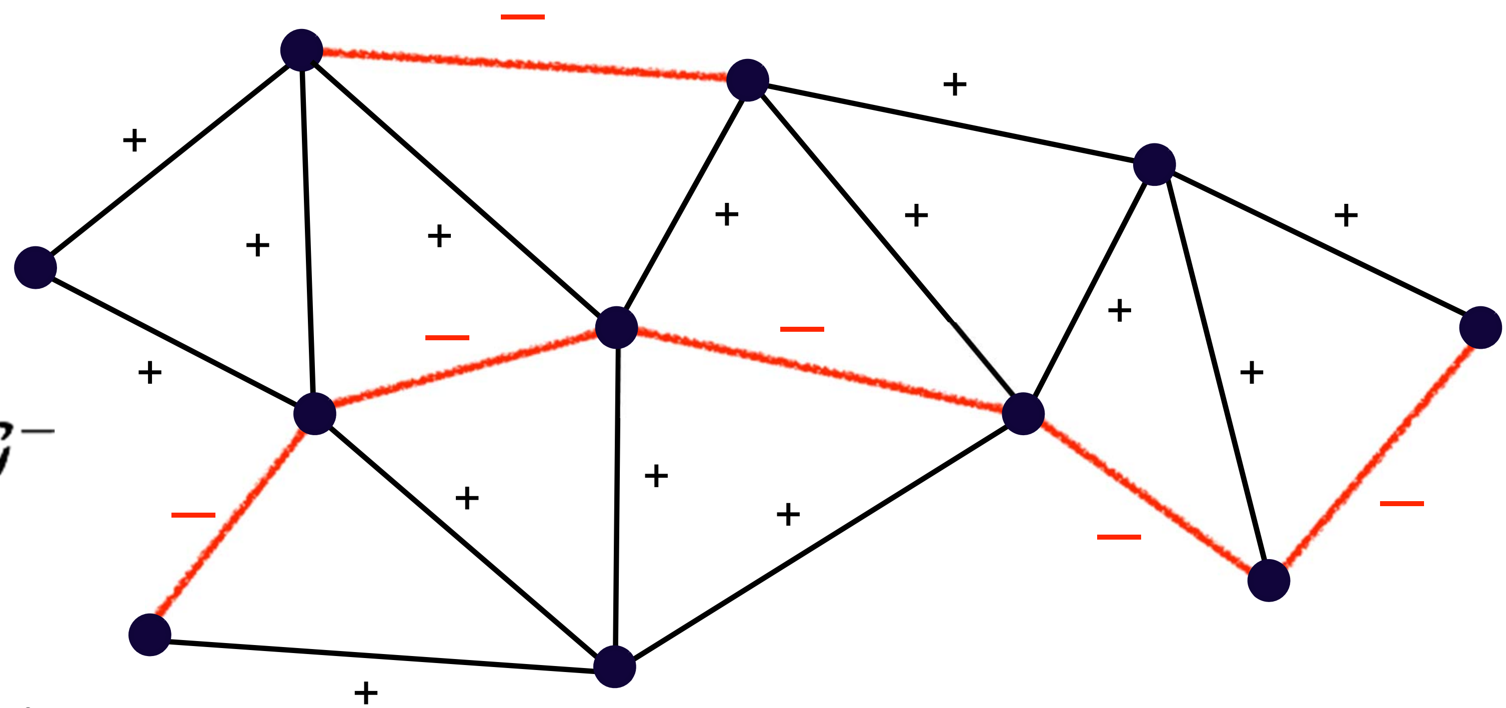
- Engineered control and algorithms for collective tasks such as optimization, formation, coverage, estimation, and filtering.

- Social and biological modeling to peer behavior in a society or in a group.

Nodes are cooperative and rational!

But are they?

Signed Networks

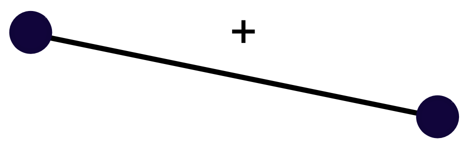


$$\mathcal{G} = \mathcal{G}^{+} \cup \mathcal{G}^{-}$$

- Fixed
- Undirected
- Deterministic
- Connected

$$\mathcal{N}_i = \mathcal{N}_i^{+} \cup \mathcal{N}_i^{-}$$

Positive Dynamics



$$x_i(k+1) = x_i(k) + \alpha\big(x_j(k) - x_i(k)\big)$$

- Classical DeGroot's rule for opinion update between two trustful individuals in a social network.

- Foundation of many distributed engineering solutions e.g., Jadbabaie et al. 2003, Nedich et al. 2009, Kar and Moura 2013, etc.

Negative Dynamics

- State-Flipping Model (Altafini 2013 TAC)

$$x_i(k+1) = x_i(k) + \beta\big(-x_j(k) - x_i(k)\big)$$

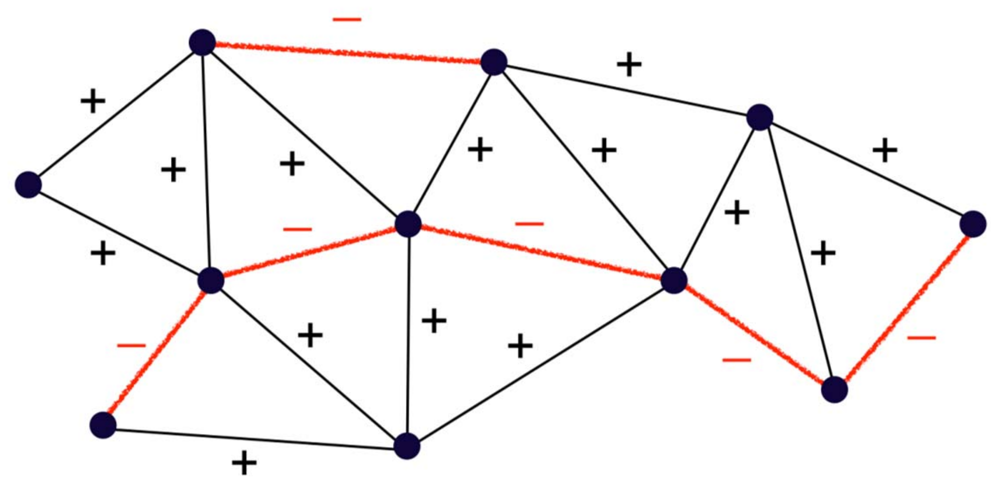
- Relative-State-Flipping Model (Shi et al. 2013 JSAC)

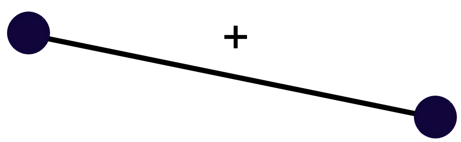
$$x_i(k+1) = x_i(k) + \beta\big(x_i(k) - x_j(k)\big)$$

The Institute for Systems Research

State-Flipping Model

UNIVERSITY OF MARYLAND 1856





$$x_i(k+1) = x_i(k) + \alpha\big(x_j(k) - x_i(k)\big)$$

$$x_i(k+1) = x_i(k) + \beta\big(-x_j(k) - x_i(k)\big)$$

State-Flipping Model

Lemma. Let $\alpha|\mathcal{N}_i^+| + \beta|\mathcal{N}_i^-| < 1$ for all i. For any initial value $\mathbf{x}_0$, there exists $\mathbf{y}(\mathbf{x}_0)$ with $\mathbf{A}\mathbf{y} = \mathbf{y}$ such that

$$\lim_{k\to\infty} x_i(k) = y_i, \ i = 1, \dots, N.$$

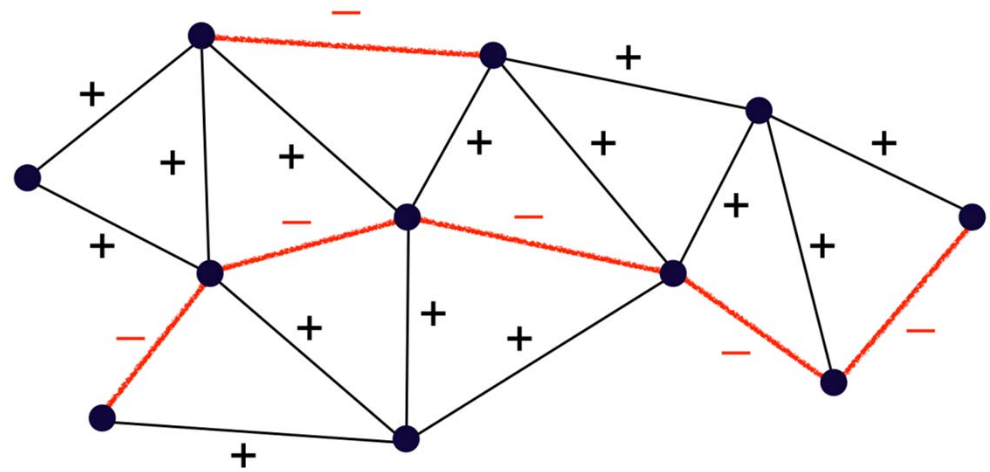
Theorem. (i) If $\mathcal{G}$ is strongly balanced, then there is a partition of the node set $\mathcal{V}$ into $\mathcal{V}_1$ and $\mathcal{V}_2$ such that

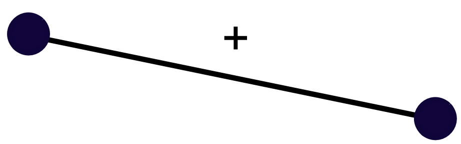
$$\begin{aligned} y_i &= y_*, \quad i \in \mathcal{V}_1; \\ y_i &= -y_*, \quad i \in \mathcal{V}_2. \end{aligned}$$

(ii) If $\mathcal{G}$ is not strongly balanced, then $y_i = 0$ for all i.

A signed graph is **strongly balanced** if the node set can be divided into two disjoint subsets such that negative links can only exist between them; **weakly balanced** if such a partition contains maybe more than two subsets.

Relative-State-Flipping Model





$$x_i(k+1) = x_i(k) + \alpha\big(x_j(k) - x_i(k)\big)$$

$$x_i(k+1) = x_i(k) + \beta\big(x_i(k) - x_j(k)\big)$$

Relative-State-Flipping Model

Theorem. Suppose $\mathcal{G}^+$ is connected and $\mathcal{G}^-$ is non-empty. Let $\alpha|\mathcal{N}_i^+| < 1$. Then there exists β_* such that
(i) if $\beta < \beta_*$,

$$\lim_{k\to\infty} x_i(k) = \frac{\sum_{j=1}^N x_j(0)}{N}, i = 1, \ldots, N;$$

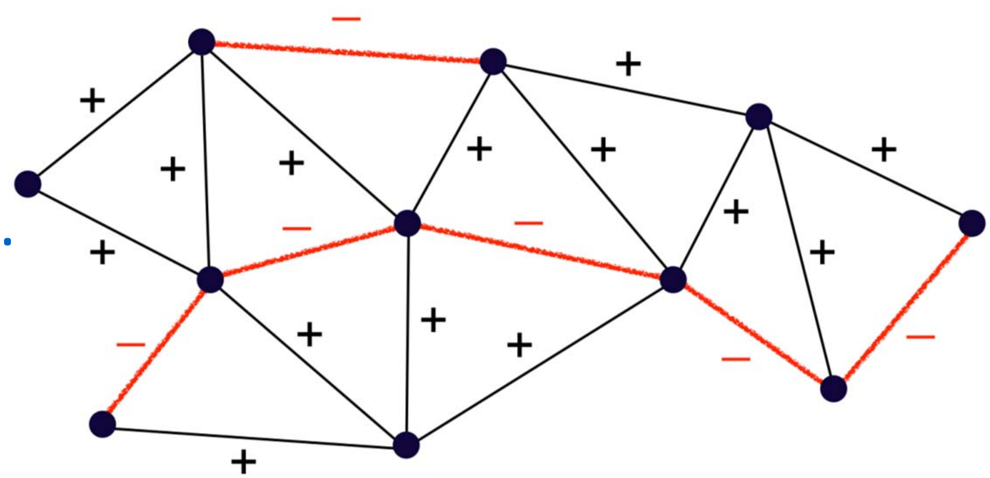
(ii) if $\beta > \beta_*$,

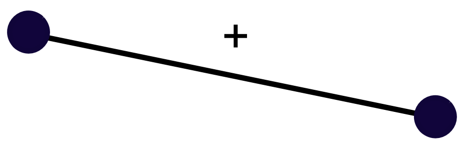
$$\lim_{k\to\infty} \|\mathbf{x}(k)\| = \infty$$

for some initial values.

Random Signed Graphs

A pair (i,j) is randomly selected.
The two selected nodes update.



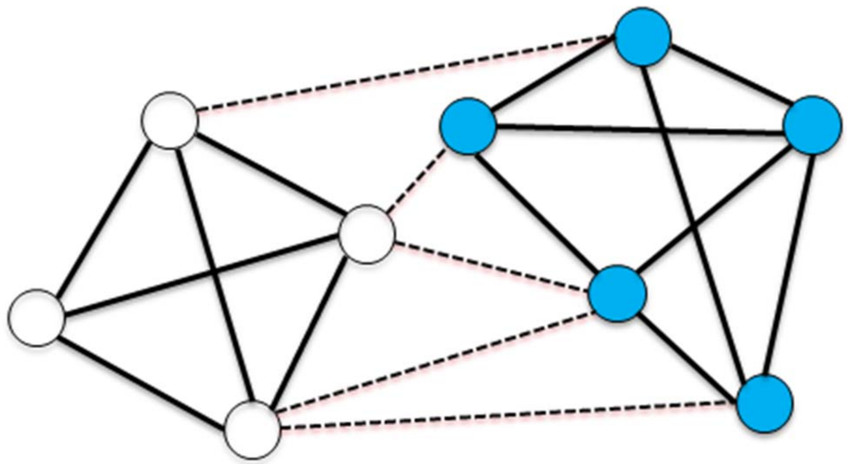


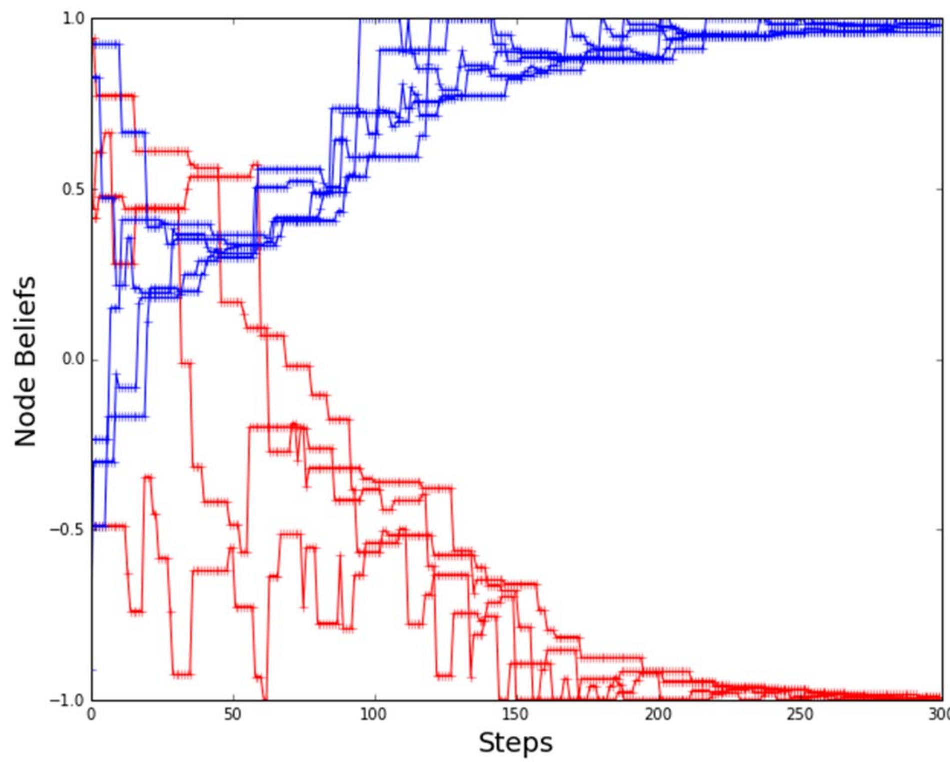
$$x_i(k+1) = x_i(k) + \alpha\big(x_j(k) - x_i(k)\big)$$

S-F Model $$x_i(k+1) = x_i(k) + \beta\big(-x_j(k) - x_i(k)\big)$$

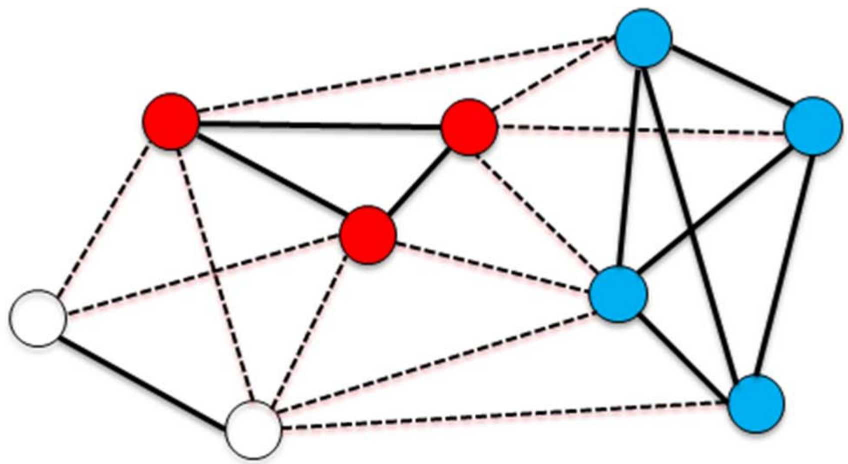
R-S-F Model $$x_i(k+1) = x_i(k) + \beta\big(x_i(k) - x_j(k)\big)$$

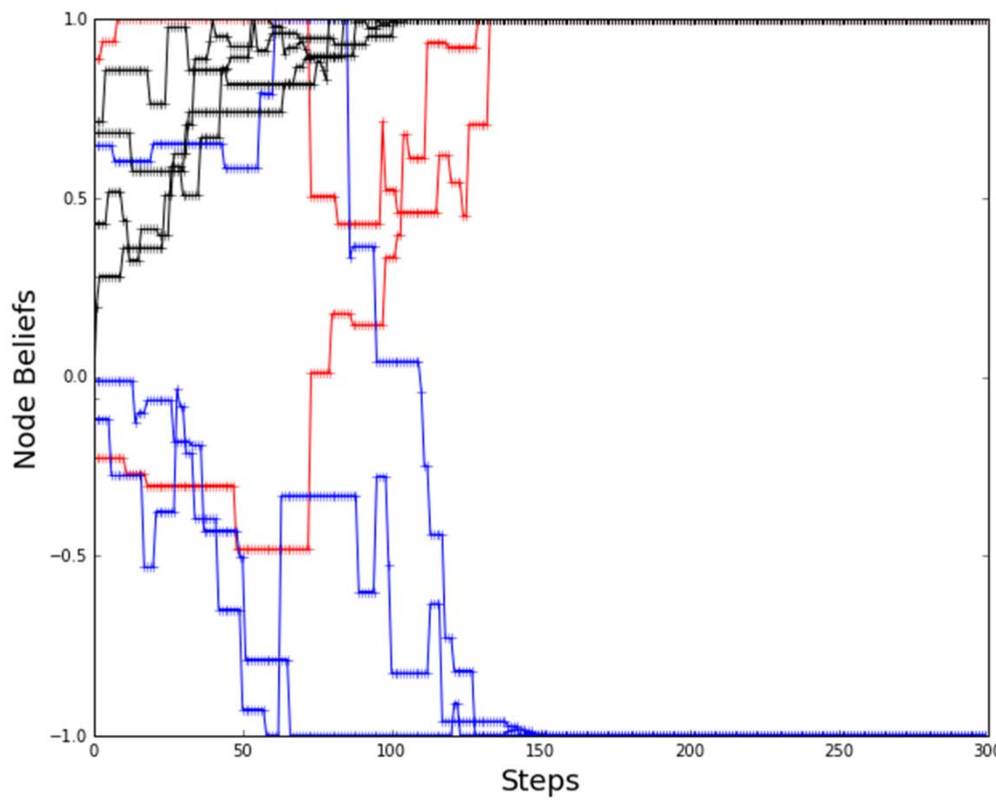
Relative-State-Flipping Model



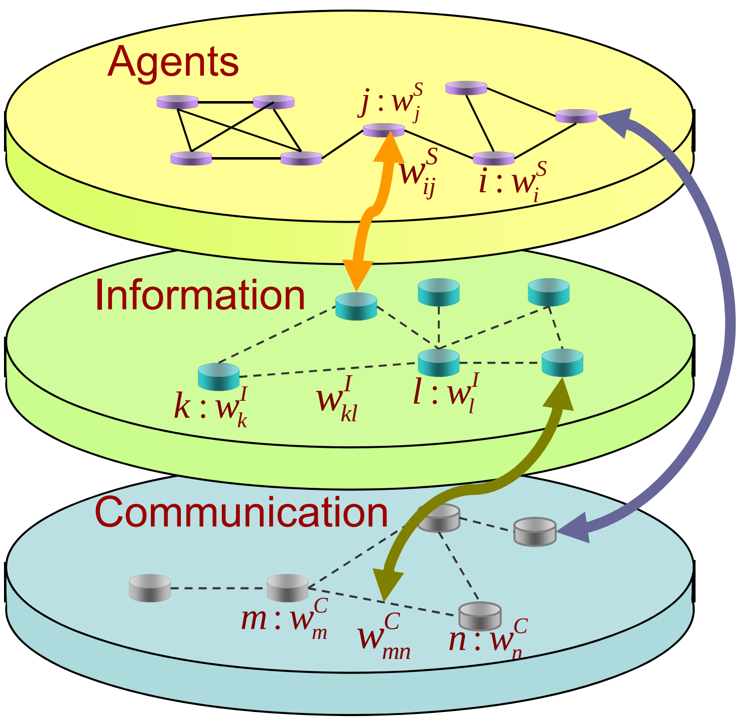


Relative-State-Flipping Model





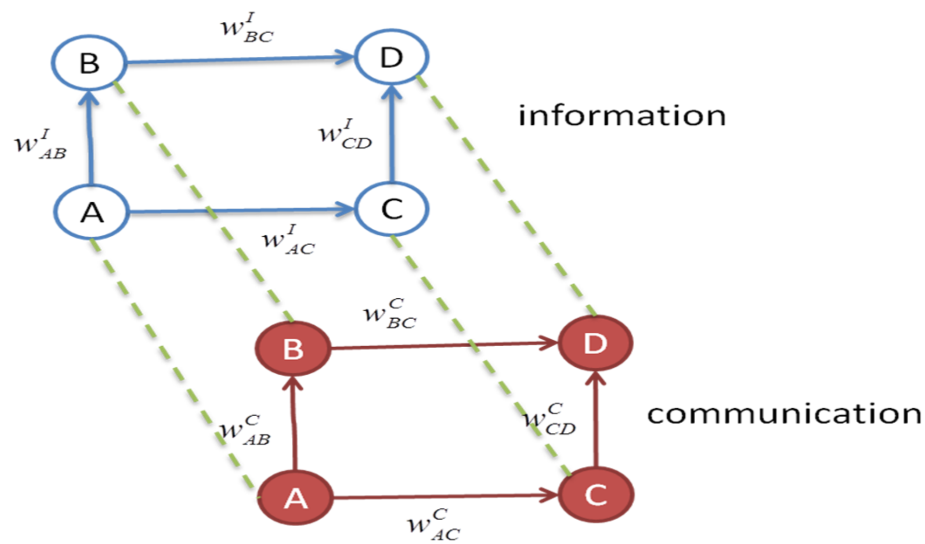
Composite Trust: Value Directed Graphs



- Value directed multi-graphs with weighted nodes
  - Inspired by advanced dynamic network models and trust research in social networks
  - Directed graphs with weights on their links and nodes
  - Weights represent trust metrics on both links and nodes

Example

- A two-level graphs with trust weights



  - Information semiring is <W^I, max, min, 0, 1>
  - Communication semiring is <W^C, max, min, 0, 1>
  - Trust semiring is TS=<$W^I \times W^C$, $+_{trust}$, $\times_{trust}$, 0, 1>

Example (cont.)

- Two different set of constraint preferences
  - Information preferred

$$(w_1^I, w_1^C) +_{trust} (w_2^I, w_2^C) = \begin{cases} (w_1^I, w_1^C) & if\ w_1^I > w_2^I \\ (w_2^I, w_2^C) & if\ w_1^I < w_2^I \\ (w_1^I, \max(w_1^C, w_2^C)) & if\ w_1^I = w_2^I \end{cases}$$

$$(w_1^I, w_1^C) \times_{trust} (w_2^I, w_2^C) = (\min(w_1^I, w_2^I), \min(w_1^C, w_2^C))$$

  - Communication preferred

$$(w_1^I, w_1^C) +_{trust} (w_2^I, w_2^C) = \begin{cases} (w_1^I, w_1^C) & if\ w_1^C > w_2^C \\ (w_2^I, w_2^C) & if\ w_1^C < w_2^C \\ (\max(w_1^I, w_2^I), w_1^C) & if\ w_1^C = w_2^C \end{cases}$$

$$(w_1^I, w_1^C) \times_{trust} (w_2^I, w_2^C) = (\min(w_1^I, w_2^I), \min(w_1^C, w_2^C))$$

Example (cont.)

- This specific trust SCSP has a distributed solution where the following algorithm is carried out at every node in the network

Algorithm: The distributed solution to solve the SCSP.

Repeat

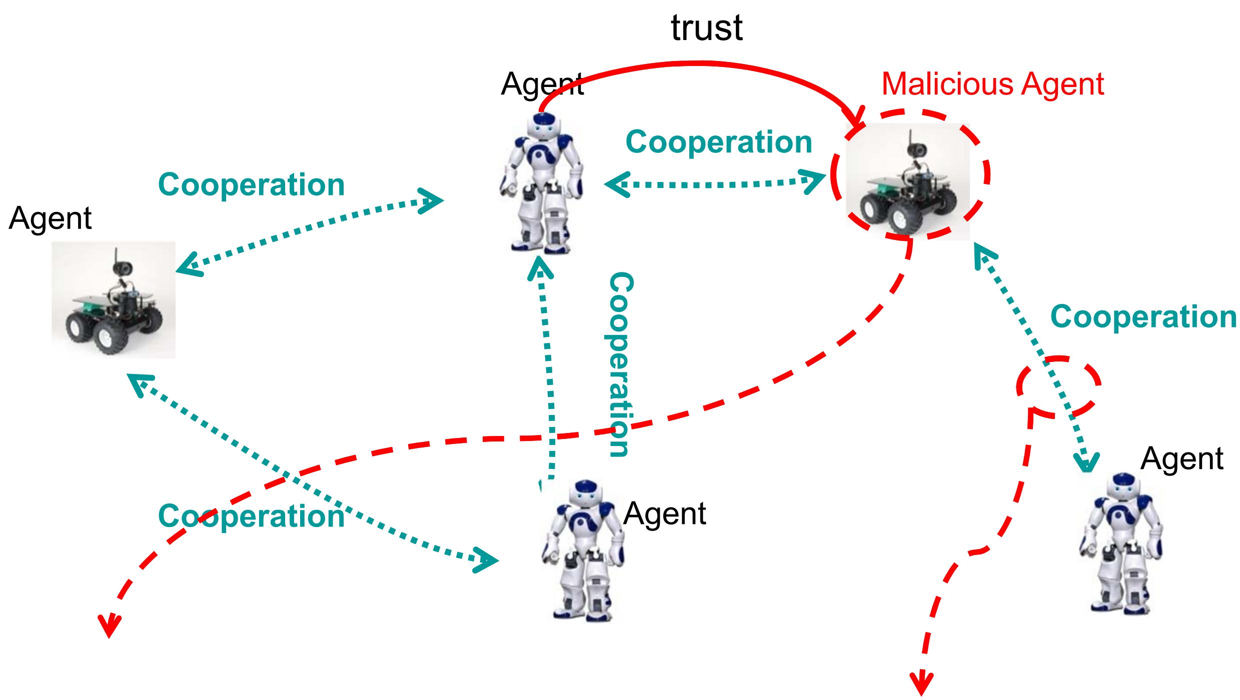
$$X_k^{n+1}(D) = \sum_{l \in \mathbb{N}_k} w_{kl} \times_{trust} X_l^n(D)$$

Until $X_k^n(D)$ converges.

  - $X_l^n(D)$ represents the evaluated trust to target D via a chain of n direct trust relations
  - $\sum = +_{trust}$

Consensus with Adversaries

- Solve the problem via detecting adversaries in networks of low connectivity.
- We integrate a trust evaluation mechanism into our consensus algorithm, and propose a two-layer hierarchical framework.
  - Trust is established via headers (aka trusted nodes)
  - The top layer is a super-step running a **vectorized consensus algorithm**
  - The bottom layer is a sub-step executing our **parallel vectorized voting scheme**.
  - Information is exchanged between the two layers – they **collaborate**
- We demonstrate via examples solvable by our approach but not otherwise
- We also derive an upper bound on the number of adversaries that our algorithm can resist in each super-step



Malicious agent:

- Multiparty secure computation

[4] Garay, Juan A., and Rafail Ostrovsky. "Almost-everywhere secure computation." Advances in Cryptology–EUROCRYPT 2008.

- Consensus with Byzantine adversaries (System theory)

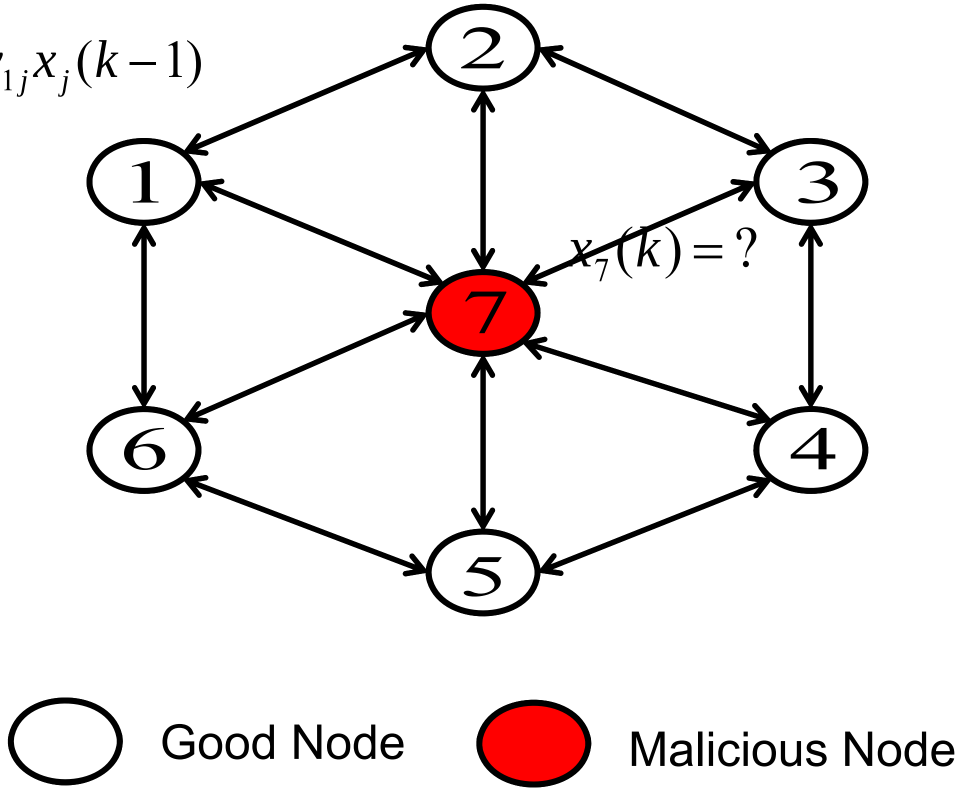
[5] Pasqualetti, Fabio, Antonio Bicchi, and Francesco Bullo. "Consensus computation in unreliable networks: A system theoretic approach," IEEE TAC, 2012.

Link Jam & Noise Injection:

[3]Khanafer, Ali, Behrouz Touri, and Tamer Basar. "Consensus in the presence of an adversary." 3rd IFAC Workshop on Distributed Estimation and Control in Networked Systems (NecSys). 2012.

Problem Formulation – Simple Example

$$x_1(k) = \sum_{j \in N_1} w_{1j} x_j(k-1)$$



Goal:

Detect malicious nodes and isolate them from consensus algorithm.

Problem Formulation (cont.)

- Without considering failures, for certain nodes, the consensus problem in distributed control can be solved by simply iteratively calculating weighted averages of nodes' neighboring states.
  - Network of agents modeled by directed graph $G(k) = (V;E(k))$

    V denotes the set of nodes and $E(k)$ the set of edges at time k

    $N_i(k) = \{j \mid e_{ij}(k) \in E(k), j \neq i\}$ set of neighbor nodes of i

    "can hear from at time k". $N_i^+(k) = N_i(k) \cup \{i\}$
  - Nodes' states (decisions, beliefs, opinions, etc.) evolve in time according to the dynamics:

$$x_i(k) = \sum_{j \in N_i(k)} w_{ij}(k) x_j(k-1) + w_{ii}(k) x_i(k-1)$$

$X(k) = \{x_1(k), x_2(k), \ldots, x_N(k)\}^T$ N-dimensional vector of nodes' states at time k.

$W(k)$ is the updating matrix (weight matrix) at time k, rows sum to 1.

Problem Formulation (cont.)

- Several different strategies have been proposed to solve the problem of distributed consensus with Byzantine adversaries.
- Related works rely on strong conditions on network topology:

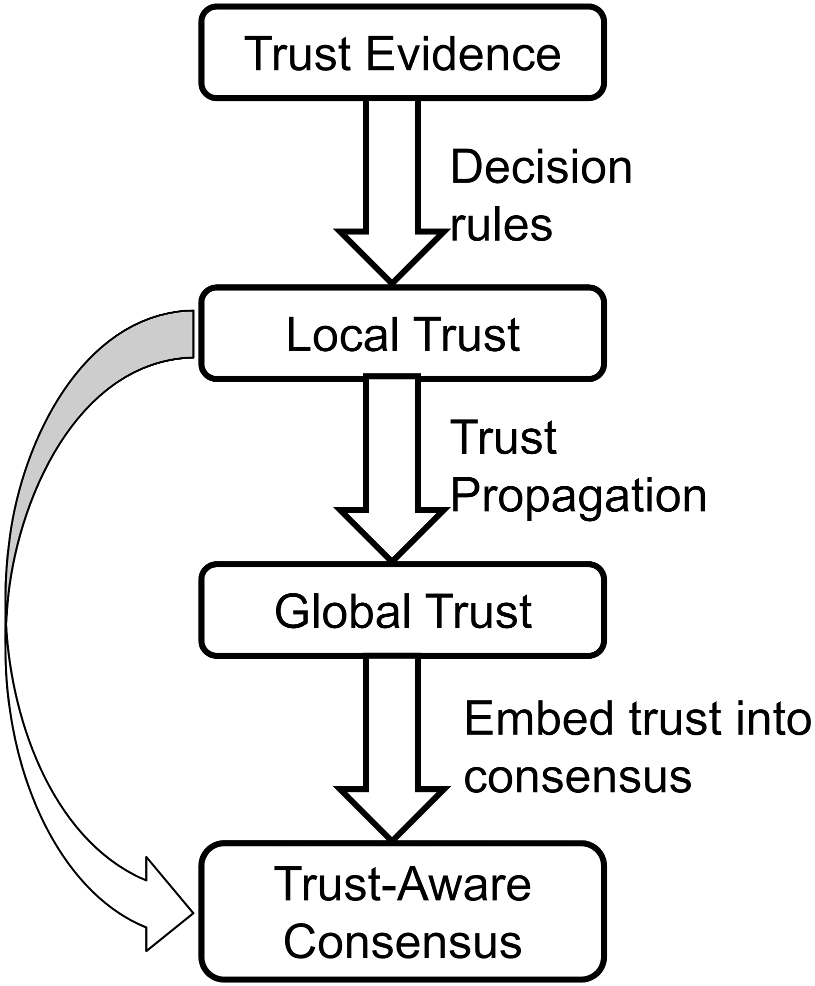
$$c \geq 2 f_b + 1$$

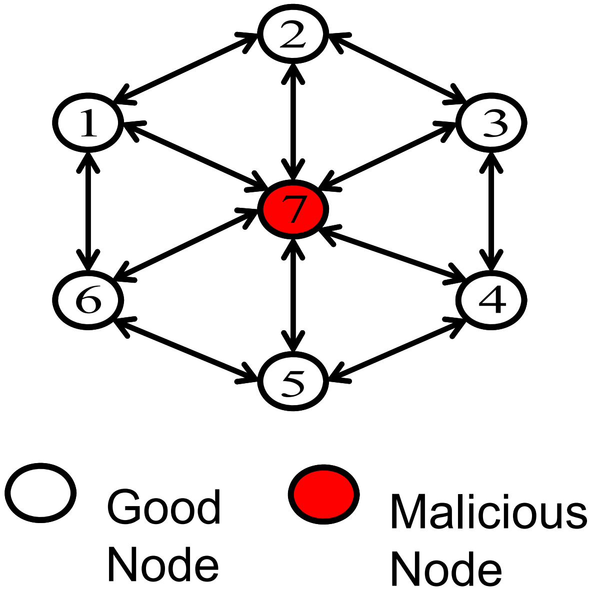
$$n \geq 3 f_b$$

  - $c = \min\{c_{ij,} \forall i, j \in V, i \neq j\}$ is the **connectivity of the network**,
    c_{ij} is the number of disjoint paths between node i and node j.
  - f_b is the number of Byzantine attackers, n is the number of nodes.

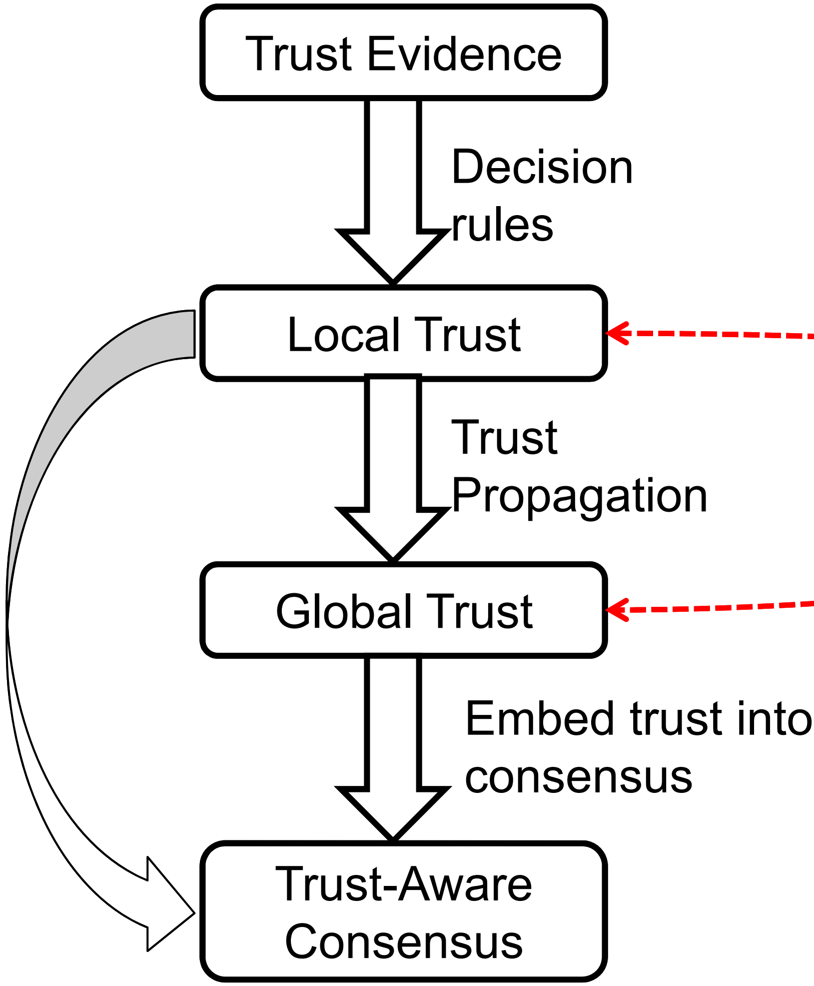
- However, these conditions about network connectivity used in related and past works cannot be verified in many situations.

Trust-Aware Consensus





Trust-Aware Consensus

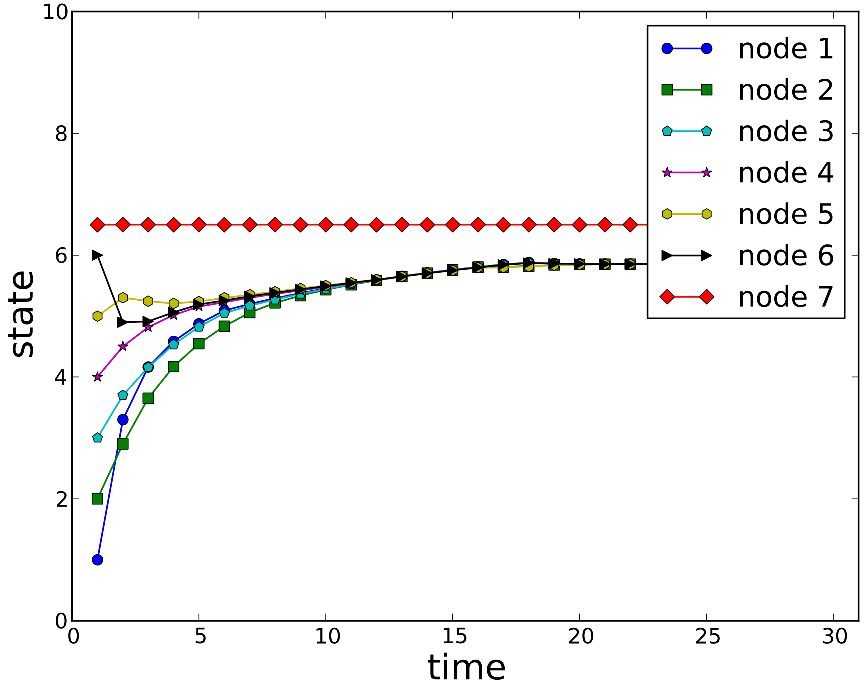


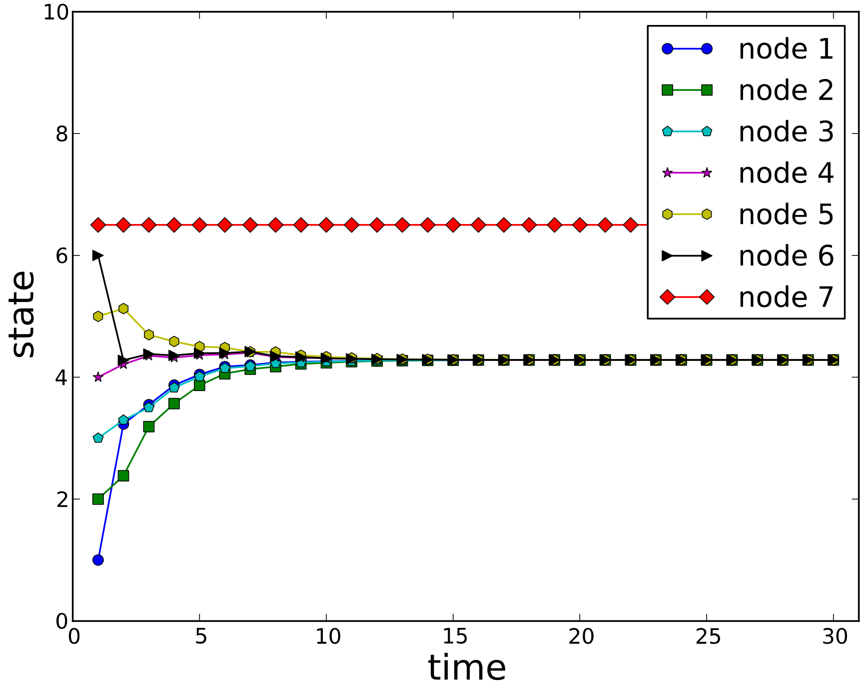
$$x_i(k) = \frac{1}{A_i(k)} \sum_{j \in N_i} t_{ij}(k) x_j(k-1)$$

$$A_i(k) = \sum_{j \in N_i} t_{ij}(k)$$

$t_{ij}(k)$ is "equilibrium" global trust values

Simulations





Adversary outputs constant message. Figure on the left has no trust propagation. Figure on the right has trust propagation.

Networked Systems – Fundamental Problems

- *Interaction between information and control*
  - controllers communicate via “signaling strategies”
  - “information neighborhoods” for controllers
  - cost of information versus cost of control
- There does not exist todate a satisfactory formulation of the joint “optimization” problem in information flow and control
- Important to develop theories that treat control strategies and information patterns in a balanced manner
- *Interactions between measurements by different agents and between system dynamics and measurements*
  - Akin to very strong interaction between information and control
  - Often the case where one cannot prove existence of an optimal control law (or design)

Simpler Problem: Information Retrieval (IR)

- Relevance is subjective – varies from user to user
- Relevance depends on the state of the user – but it changes as user acquires information
- Plenty of evidence that relevance of a document to a user changes as the user interacts with the system
- Probabilistic assessment of relevance – **but on what event logic**?
- Ample experimental evidence : IR based on current Boolean model does not deliver required performance (Van Rijsbergen, 2006)

Non-commutative Probability Examples

- Tracking and identification of moving objects using multiple-cameras
- High-level activity detection and anomalous activity mining from multiple perspectives
- Trust in social networks
  - Neuropsychological studies, emotional activation, interpersonal relationships, trust, decisions relying on trust.
- Human judgments and noncommutativity
  - Based on indefinite state, create than record, disturb each other, do not obey classic logic, law of total probability does not hold

Non-commutative Probability Examples

- Human cognition and decision making
  - Disjunction effect
  - interference between categorizarion and decision making
  - Conjunction fallacy
  - Compositionality in the semantics of cognitive information processing
  - Related to question order effects that cannot be explained by classical probability models
- Classical Kolmogorov-like models cannot explain any of the observed phenomena and measurements, in examples.
- Recent studies utilizing the alternative quantum-like probabilities and logics have shown considerable agreement with the experimental data in these phenomena

Multi-Agent Networked Systems: Event-State-Operation Structures

- Multi-agent system – incompatible events – occurrence cannot be verified by two or more agents
- Manifestation of communication constraints – or interactions
  - Sensor networks – domain of observation or sensor range
  - Multi-agent control – domain of influence or control range
- Incompatible measurements – new essential concept in multi-agent systems
- Need to build probabilistic models that have incompatibility built-in – Conditioning and its modeling is at the center of this
- Multi-agent setting: data/measurements lead to two incompatible events – how do we describe their conjunction?
- Introduce generalizations of conditional probability and conditional expectation

Conclusions

- Three-layer Net-CPS model
- Effects of topology on distributed algorithm performance
- Fundamental tradeoff between the benefit from collaboration and the cost for collaboration – constrained coalitional games
- Trust as catalyst for collaboration
- Trust and Mistrust dynamics
- New probabilistic models – similar to the quantum mechanical ones
- For the future: More on Value of Information, Control -- Information Duality, Complexity and consequences, New Logics and Collaborative Teams, Noncommutative Probability

Thank you!

baras@isr.umd.edu

301-405-6606

http://www.isr.umd.edu/~baras

Questions?