Robustness of Complex Networks: Reaching Consensus Despite Adversarial Agents

Shreyas Sundaram
Department of Electrical and Computer Engineering and
Waterloo Institute for Complexity and Innovation

University of Waterloo
Standard Consensus Dynamics

- Network: \( n \) nodes \( \{x_1, x_2, \ldots, x_n\} \), edge set \( E \)
- Each node \( x_i \) starts with a real number \( x_i[0] \)
- **Linear averaging dynamics:**

\[ x_i[k + 1] = w_{ii}x_i[k] + \sum_{j \in \text{nbr}(i)} w_{ij}x_j[k] \]

- As long as the network is **connected**:

\[ \lim_{k \to \infty} x_i[k] = \sum_{i=1}^{n} \alpha_i x_i[0], \quad \forall i \in \{1,2, \ldots, n\} \]

- The coefficients \( \alpha_i \) are nonnegative and sum to 1
Potential for Adversarial Behavior

- What happens if some nodes *don’t follow* the averaging dynamics?
- Example: suppose some node keeps its value *constant*
Resilient Consensus Objective

- Node set partitioned into two sets: \( N \) (normal nodes) and \( A \) (adversarial nodes)
  - Sets \( N \) and \( A \) are unknown to normal nodes
  - Adversarial nodes are allowed to update their states arbitrarily
  - Normal nodes follow whatever dynamics we propose

- Consider the following (relaxed) objective:
  “All normal nodes should asymptotically reach consensus on some value that is between the smallest and largest initial values of the normal nodes”

- Adversarial nodes should not be able to bias the consensus value excessively
Local Filtering

- Natural strategy: Each normal node is “suspicious” of extreme values in its neighborhood

- Mechanism:
  - At each time-step $k$, each node $x_i$ receives values from its neighbors
  - $x_i$ removes the $F$ highest and $F$ lowest values in its neighborhood, updates its state as a convex combination of remaining values

$$x_i[k + 1] = w_{ii}x_i[k] + \sum_{j \in \text{nbr}(i)} w_{ij}x_j[k]$$

- $F$ is a parameter indicating level of suspicion

Neighbors after removing extreme values
Convergence

- Traditional graph metrics not useful to characterize convergence

- Connectivity of graph is \( n/2 \), but no node ever uses a value from opposite set
**Insufficiency of Connectivity as a Metric**

- **Connectivity is no longer a sufficient metric** to characterize behavior of purely local filtering mechanism
  - Graph contains sets where no node in any set has **enough neighbors** outside the set
  - i.e., all outside information is filtered away by each node

- **Need a new topological property** to characterize conditions under which local filtering will succeed
We introduce the following definitions

- A set $S$ is *$r$-reachable* if it has a node that has at least $r$ neighbors outside the set.
We introduce the following definitions

- A set $S$ is $r$-reachable if it has a node that has at least $r$ neighbors outside the set.
Robust Graphs

- A graph is \( r \)-robust if for any two disjoint subsets, at least one of the sets is \( r \)-reachable

3-robust graph:
Pick any two subsets of nodes, at least one is 3-reachable
Robust Graphs

- A graph is \( r \)-robust if for any two disjoint subsets, at least one of the sets is \( r \)-reachable.

3-robust graph:
Pick any two subsets of nodes, at least one is 3-reachable.
The Role of Robustness in Convergence

- **Main result:** If there are at most F adversarial nodes

  Graph is \((2F+1)\)-robust

  Normal nodes will reach consensus despite actions of adversarial nodes

- **Robustness is the key metric** for purely local filtering/diffusion mechanisms

- Recall: Can construct graphs that have very high connectivity \((n/2)\), but that are only 1-robust

- Question: What is the robustness of “complex networks”?  
  - Will purely local filtering mechanisms work on these networks?

Zhang and Sundaram, ACC 2012; LeBlanc, Zhang, Koutsoukos and Sundaram, IEEE JSAC 2013; Vaidya et al., PODC 2012
Erdos-Renyi Graphs

- Erdos-Renyi graphs $G(n, p(n))$: Define

$$p(n) = \frac{\ln(n) + (r - 1) \ln \ln(n) + c(n)}{n}$$

- If $c(n) \to -\infty$ as $n \to \infty$, $G(n, p(n))$ almost surely has min degree, connectivity and robustness less than $r$ as $n \to \infty$

- If $c(n) \to \infty$ as $n \to \infty$, $G(n, p(n))$ almost surely has min degree, connectivity and robustness at least $r$ as $n \to \infty$
Phase Transition for Erdos-Renyi Graphs

- **Threshold function:**
  \[ t(n) = \frac{\ln(n) + (r - 1) \ln \ln(n)}{n} \]

- ER graph experiences a phase transition for \( r \)-min degree, \( r \)-connectivity and \( r \)-robustness at this threshold

- There is a “triple jump” at this threshold [Zhang & Sundaram, CDC 2012]

- “Double jump” for min degree and connectivity known since [Erdos & Renyi, 1961]
For 1-d geometric graphs, we show:

If graph is $\left(\frac{3}{2}r\right)$-connected, then it is at least $r$-robust

Key point: highly connected 1-d geometric random graphs are also highly robust
Preferential Attachment Networks

- One option to model graphs that grow over time: **Preferential Attachment process**

  - Start with a small group of nodes
  - At each time-step, a new node comes in and attaches to $r$ existing nodes (Barabasi-Albert model)
    - Key point: prefer to attach to nodes that have a large degree
    - Produces a power law network

- If initial network is $r$-robust, we show:
  
  Resulting Power-Law graph is $r$-connected and $r$-robust
Thanks!
(Come see poster for more details!)
Connectivity as a Metric for Robustness

- Traditional result: In fixed networks with up to F adversaries:
  - Network has at least 2F+1
  - Any two nodes can reliably exchange initial values despite actions of F adversarial nodes

- Note: adversaries allowed to update their states arbitrarily

- Requires normal nodes to know the entire network to route/decode information to/from other nodes