CERIAS

the center for education and research in information assurance and security

"Won't You Be My Neighbor?" Neighbor Selection Attacks in Mesh-based Peer-to-Peer Streaming

Jeff Seibert, David Zage and Cristina Nita-Rotaru

Department of Computer Science and CERIAS, Purdue University

P2P Video Streaming

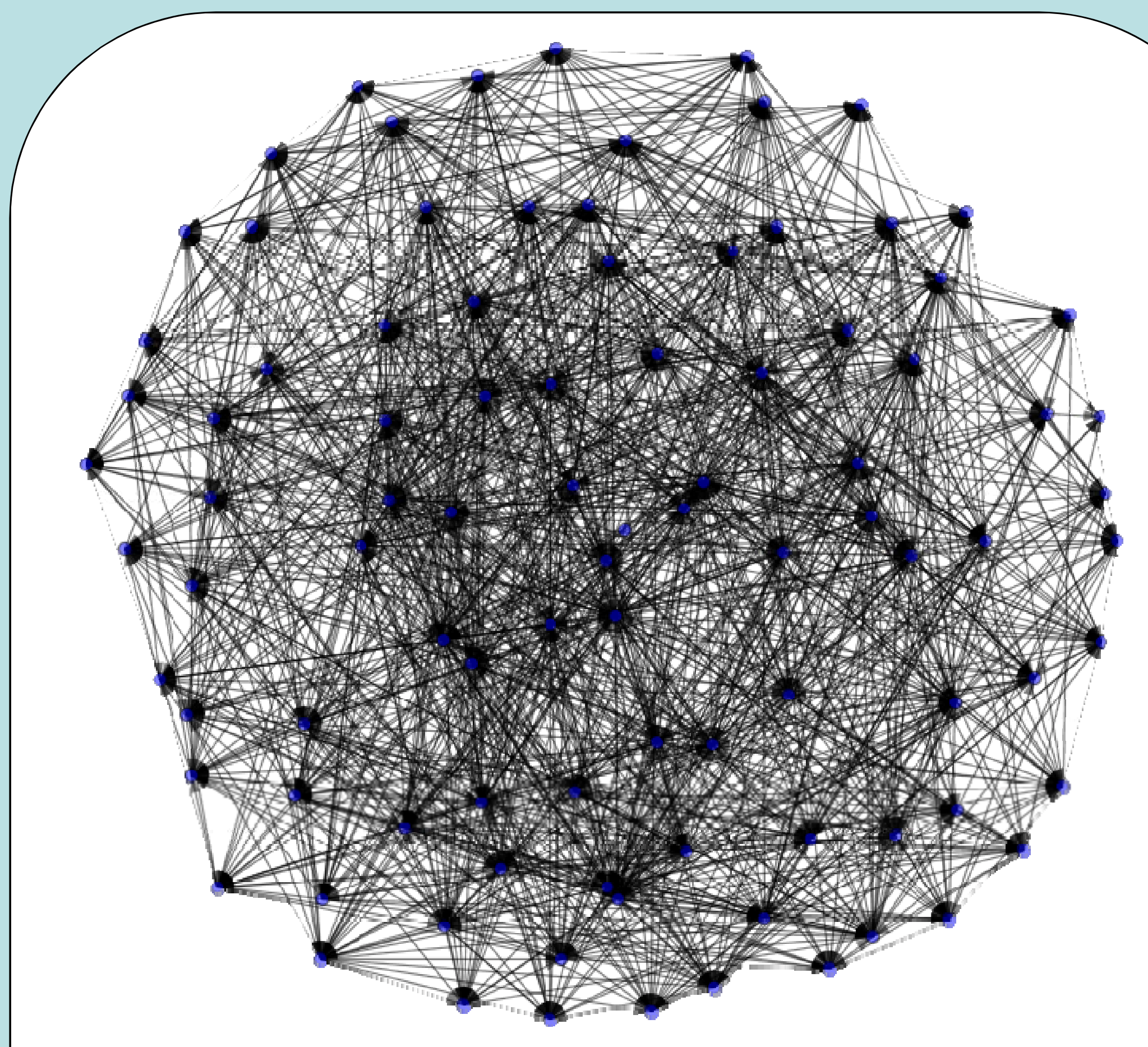
- P2P streaming is gaining interest all over the world!
  - TV anywhere in the world
  - Do not have to pay to watch
  - No extra infrastructure necessary
- Meshes have become predominant architecture of P2P streaming
  - Are resilient to churn and failures
  - Have been shown to perform better than other architectures through simulations and experiments
  - Examples: Chainsaw, CoolStreaming, PPlive and many more!

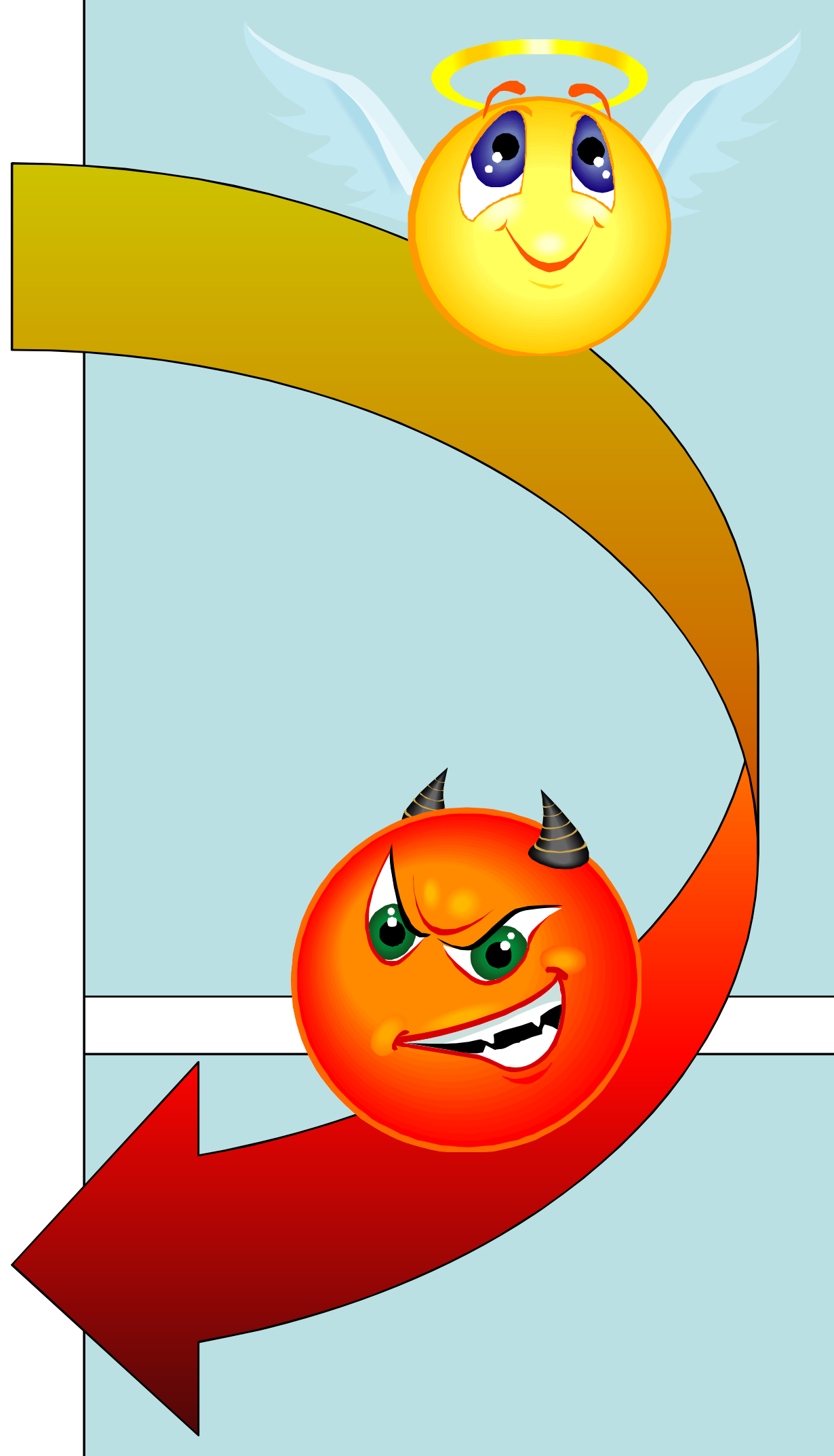
Neighbor Selection Attacks

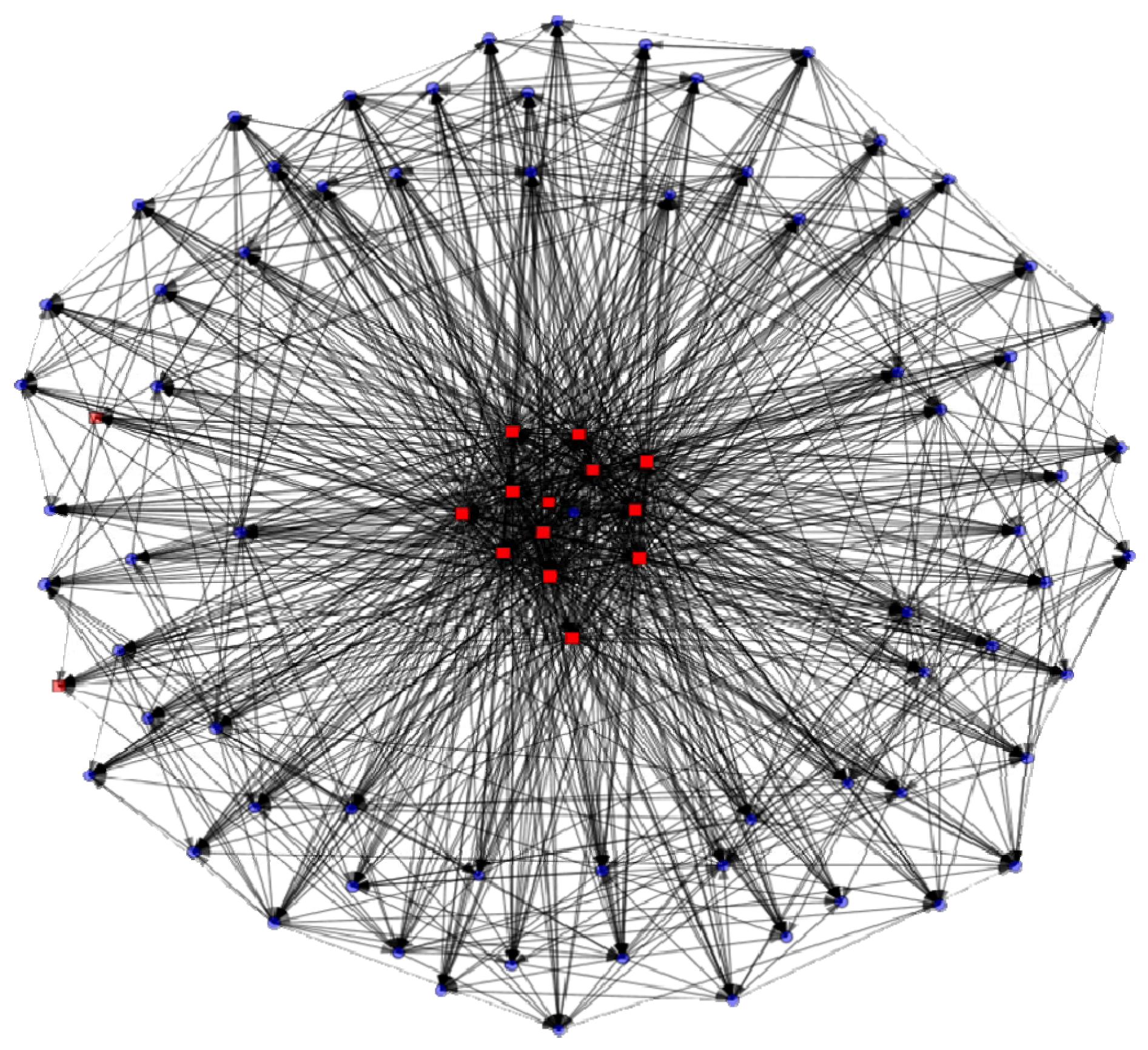
- P2P streaming systems deployments form a random mesh overlay
- Malicious nodes try to dominate the neighbor sets of benign nodes
  - Nodes in the overlay select their neighbors by referral
  - Malicious nodes can subvert the overlay building process by referring only other malicious nodes and pollute the neighbor sets of honest nodes
  - Benign nodes will also inadvertently refer malicious nodes
- This attack serves as a launching pad for other attacks
  - Traffic analysis, selective data forwarding, etc.

Mitigating the Attacks

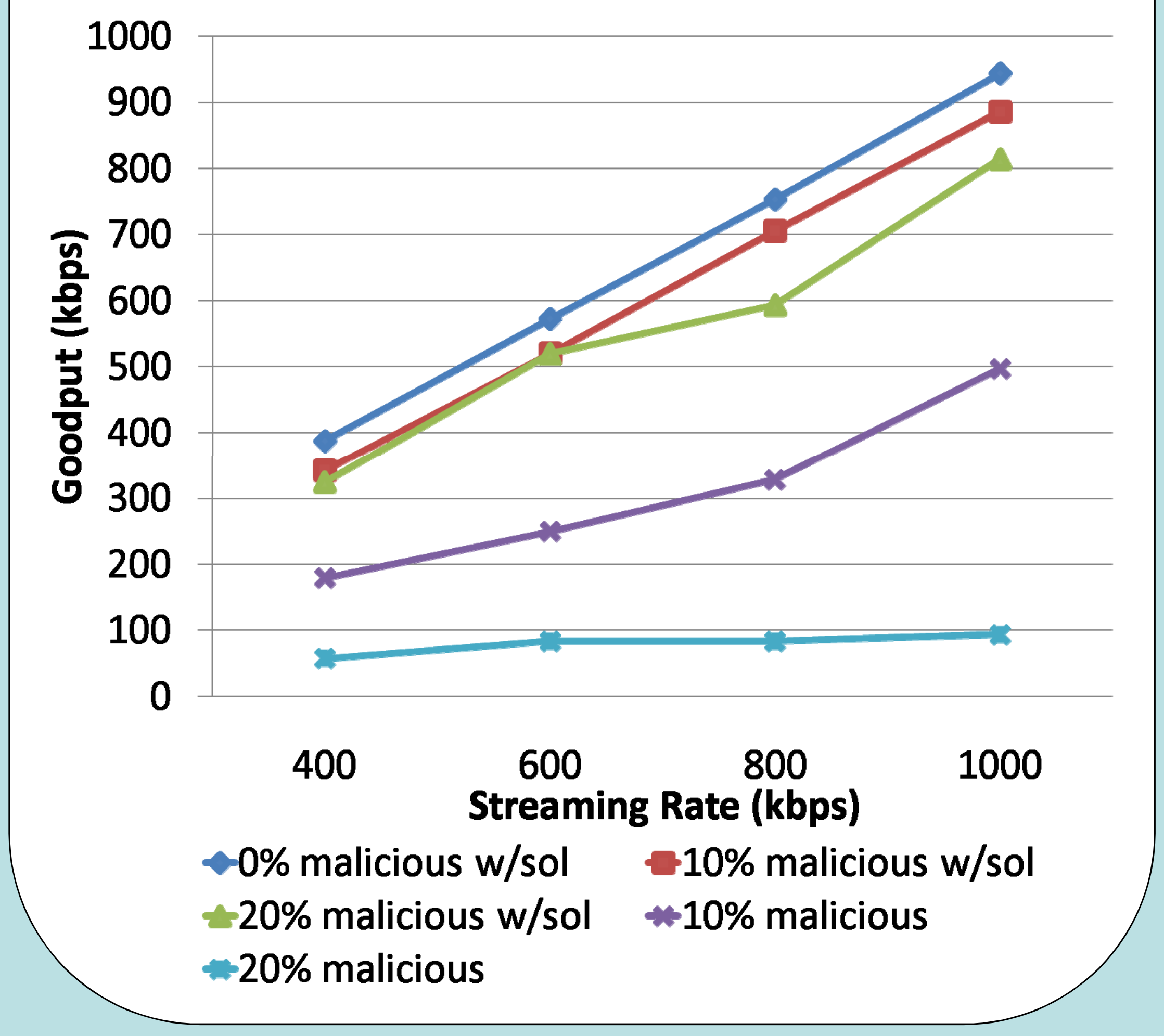
- Malicious nodes change the random graph structure of the overlay to be non-random
- We can leverage the properties of random graphs to mitigate the attack
  - Each node computes its clustering coefficient (CC) to detect when a topology is not random
  - Intuitively, CC is a measure of how connected the graph is that is formed by a node and its neighbors
  - The lower the CC is, the more random a graph is
  - If the CC is above a certain threshold, then that node disconnects the node that contributes most to its CC







Connections of a Chainsaw experiment with 100 nodes 100 seconds into an experimental run on PlanetLab. Note that in the bottom figure the presence of an attacker creates a hub of malicious nodes instead of a random graph structure as seen in the figure on the top.



Goodput on PlanetLab for an overlay of 300 nodes when malicious nodes conduct a neighbor selection attack. For demonstrative purposes, malicious nodes drop traffic going through them.

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center