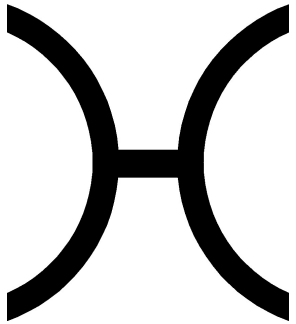
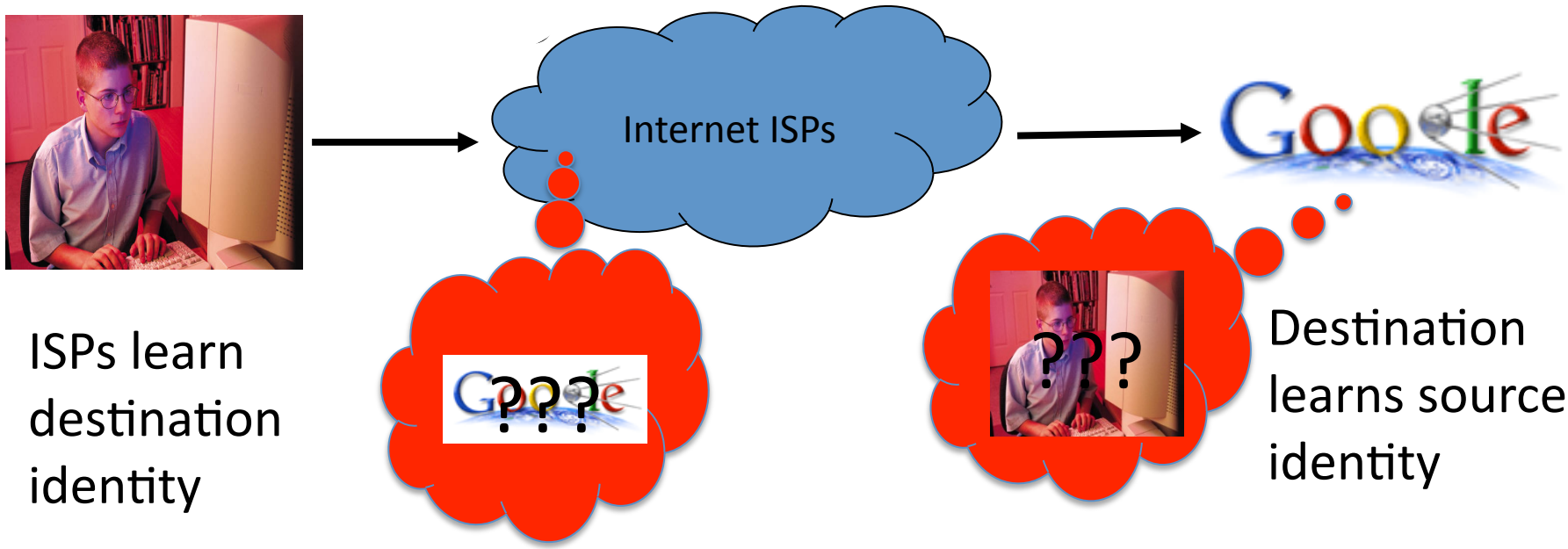


Pisces

Anonymous Communication Using Social Networks

Prateek Mittal, UC Berkeley
Matthew Wright, UT Arlington
Nikita Borisov, UIUC

Protecting Privacy with Anonymity



ISPs learn destination identity

Destination learns source identity

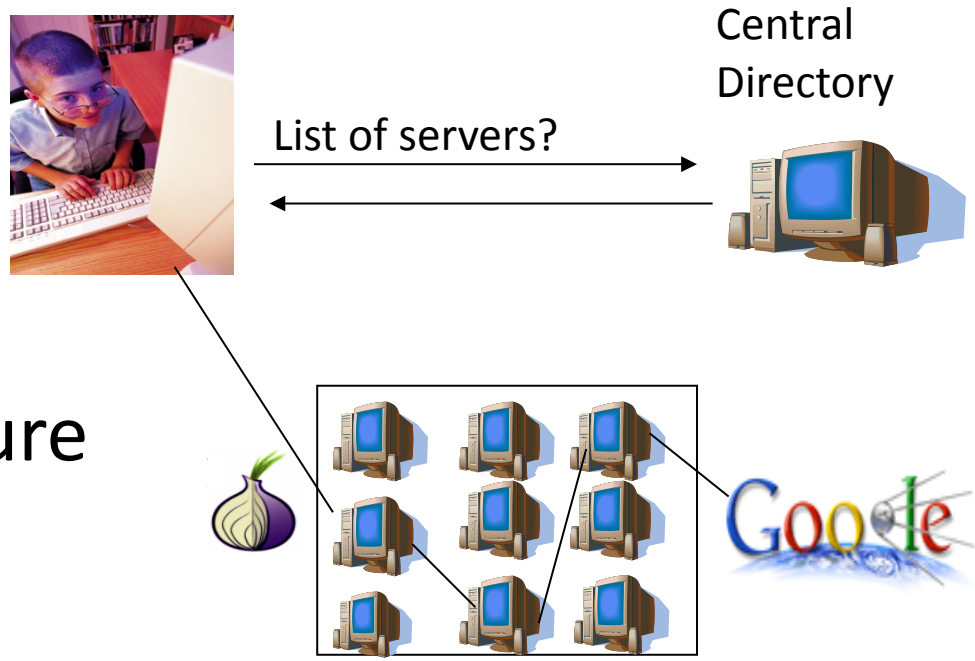
- Anonymous communication
  - Keep user identity secret from recipient or a third party.

Law enforcement
Intelligence agencies
Censorship resistance
Businesses
Citizens

Problems in Anonymity Systems (Tor)

Randomly Selected Proxies + Central Directory

- Sybil attacks
- Limited scalability
- Central points of failure

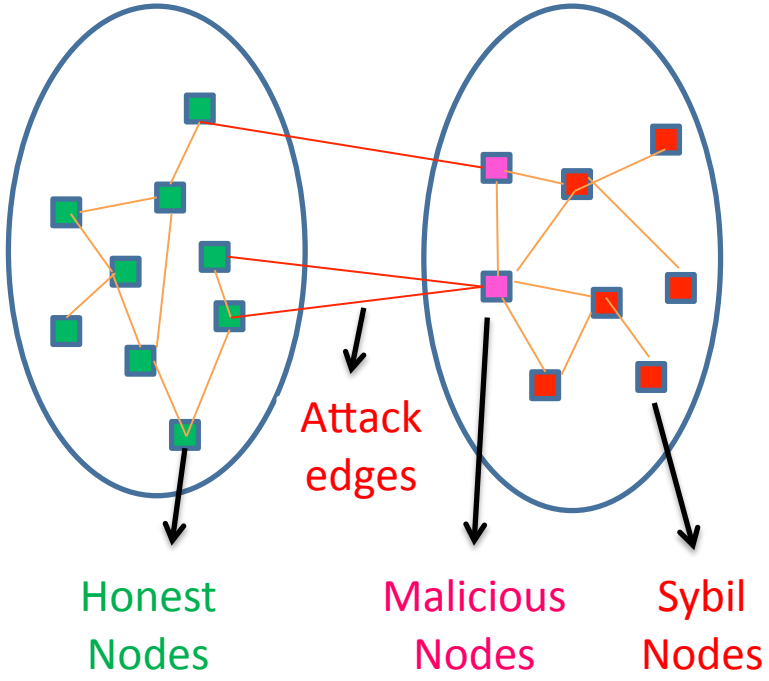


Introducing Pisces

- Leverages social trust
  - Resilience against Sybil attacks
- Scalable architecture
  - Potential for higher anonymity
- Fully decentralized approach
  - Distributed hash tables

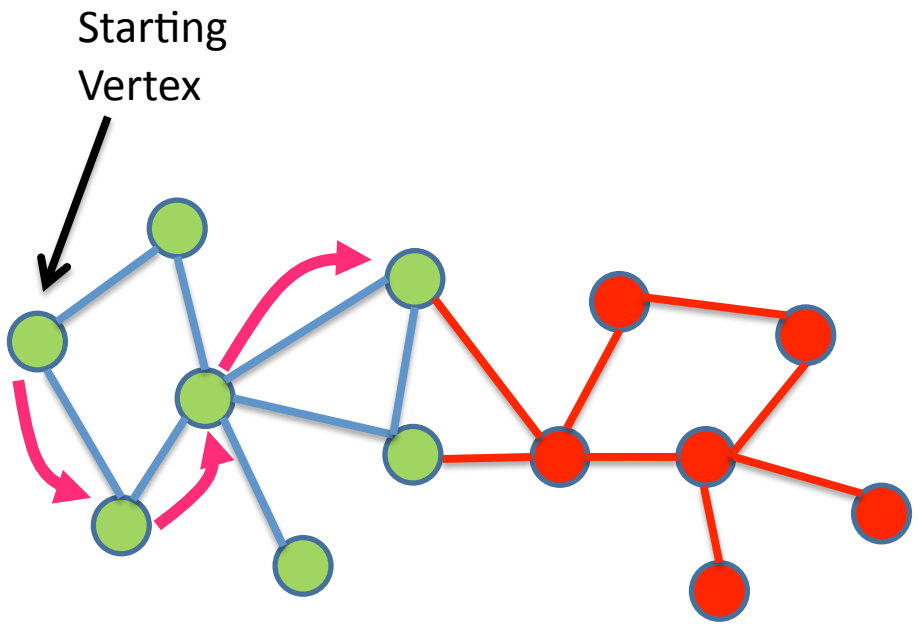
Pisces Threat Model:
Bounded Sybil Attacks in Social Networks

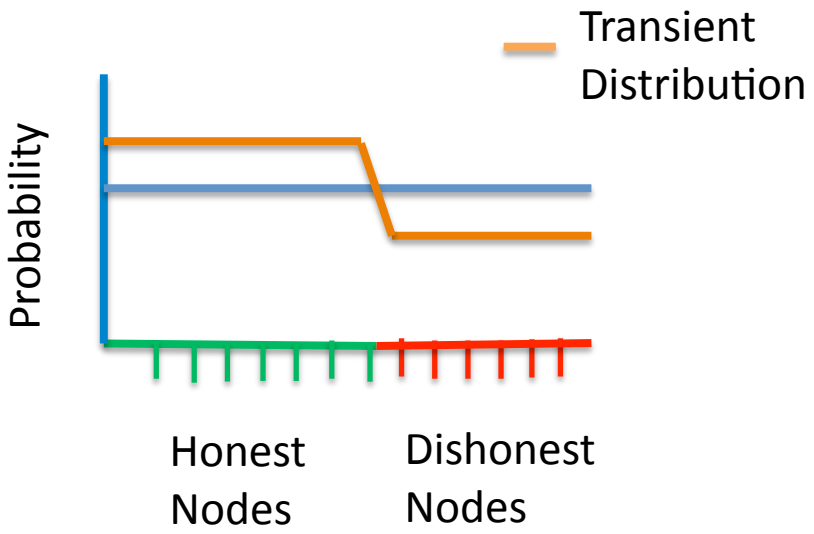
- Sybil filtering
  - Limited social engineering
  - Bound on Sybils
  - SybilLimit
- Bounded Sybils can still cause damage



Non-uniform Distribution of Adversaries

Anonymous Paths in Pisces: Leveraging Special Random Walks on Social Networks

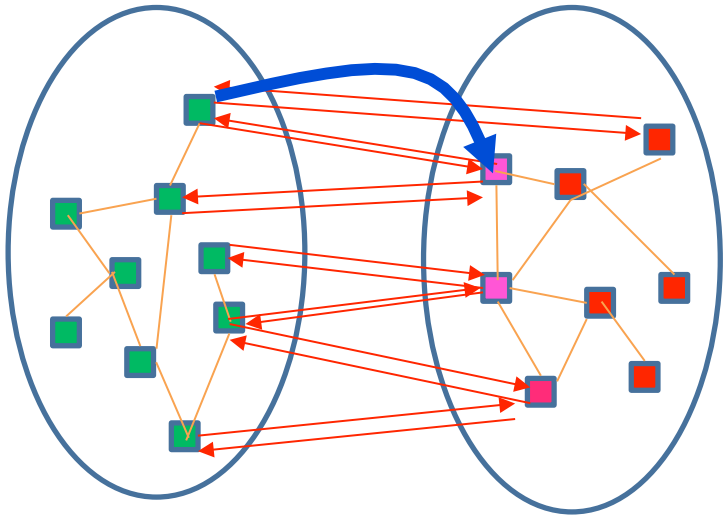




Challenge: Active Attacks on Random Walks

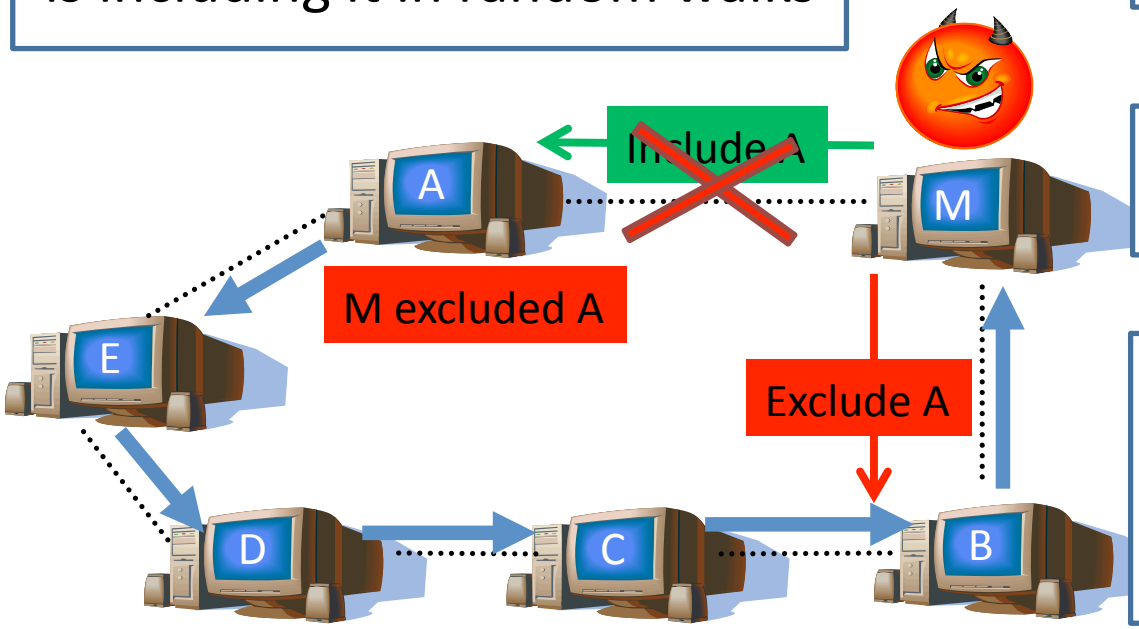
Securing Random Walks: Reciprocal Neighborhood Policy (RNP)

- Tit-for-tat policy
  - X excludes Y → Y excludes X
- Active attacks
  - → Adversary is isolated



Enforcing RNP in Pisces:
Issues with Local Attack Detection

Goal: A wants to confirm if M is including it in random walks



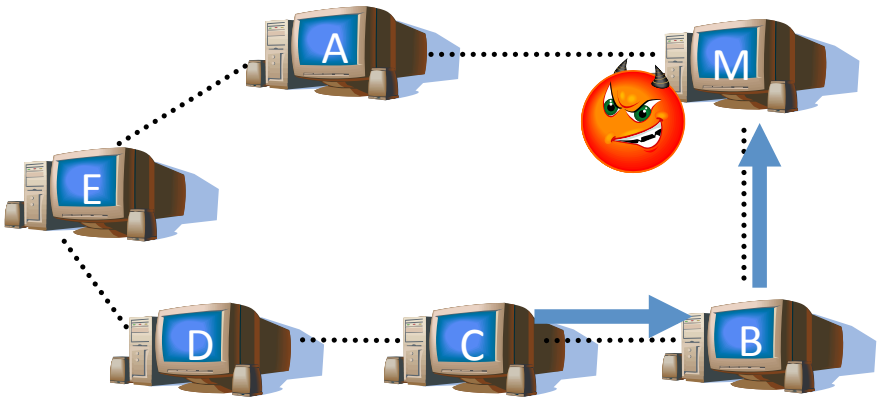
1. Variations of local querying not secure

2. A needs to query M via alternate paths (via B)

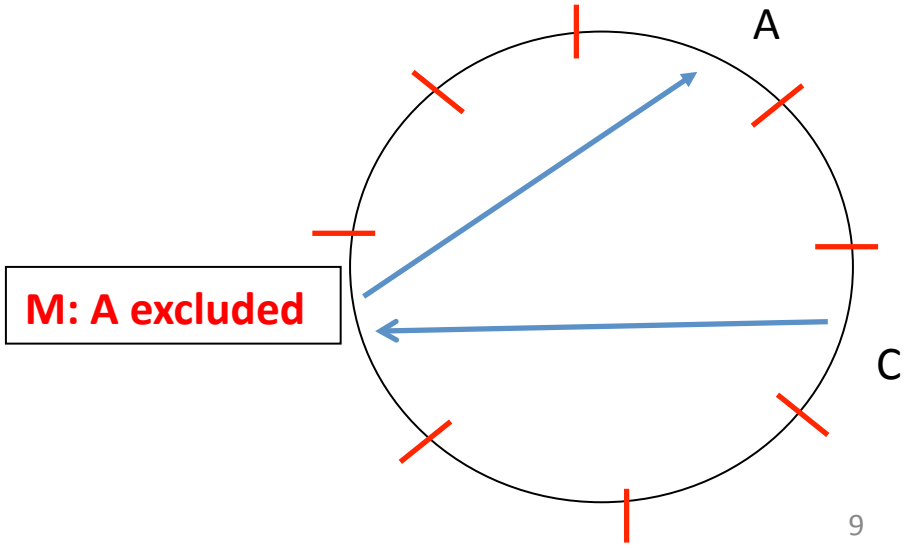
3. Unstructured topology: difficult to find alternate query paths.

Enforcing RNP in Pisces:
Collaborative Attack Detection

- Testing random walks
  - Indistinguishable from normal walks



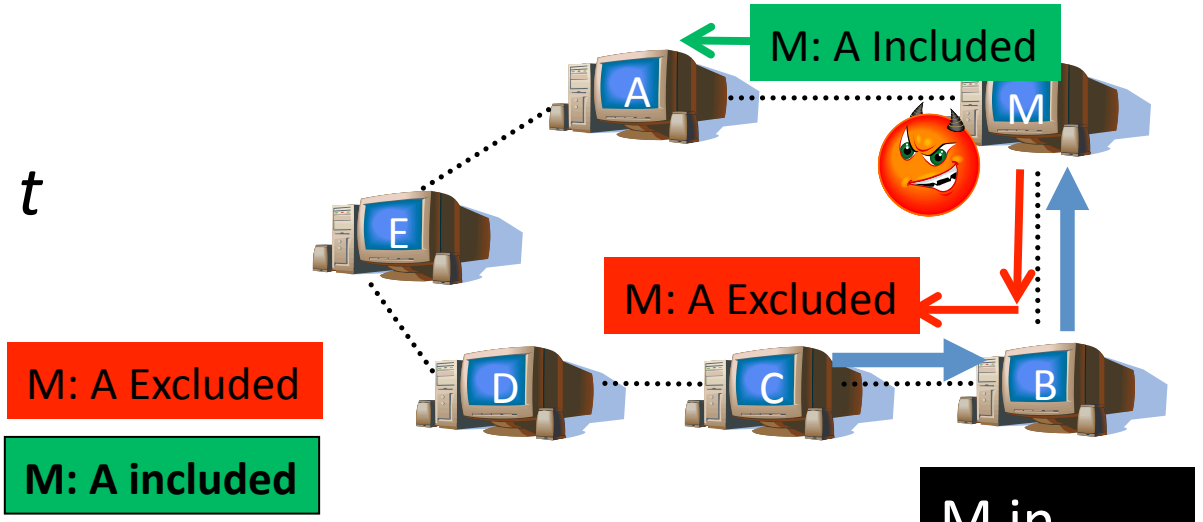
- Store results in a DHT
  - Integrity: Self-signed



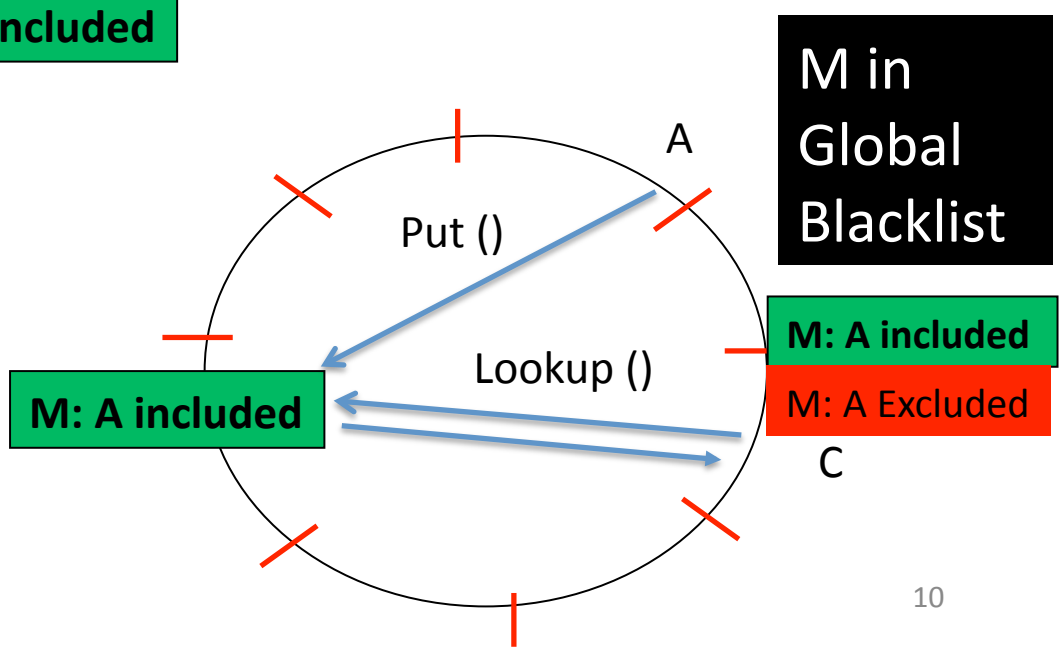
- Malicious nodes blacklisted

Enforcing RNP in Pisces: Extension to Global Blacklisting

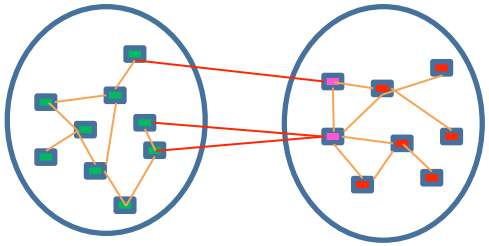
- Static friends list
  - Per time interval *t*
  - Contract

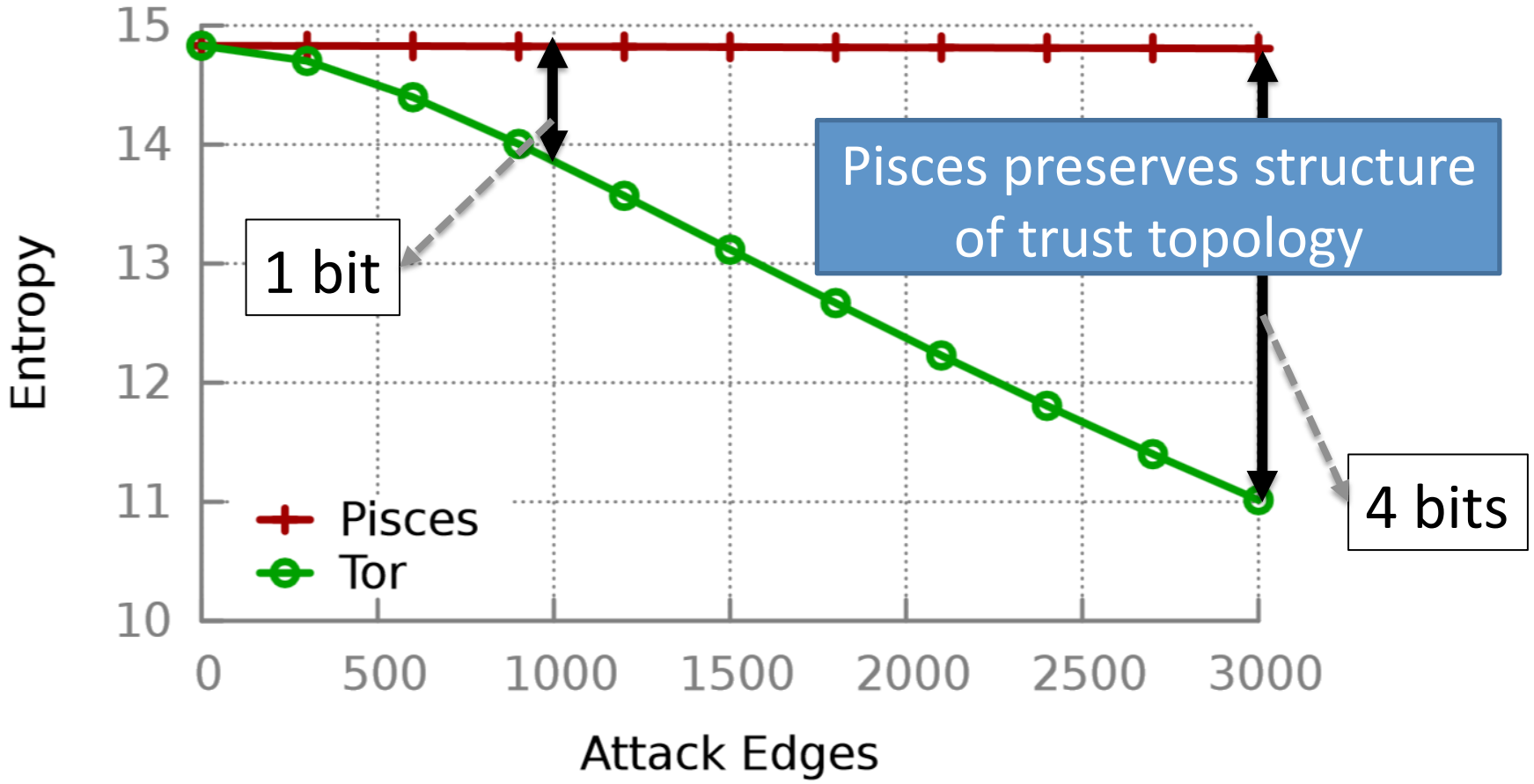


- Conflicting tables
  - Malicious behavior
  - Unforgeable proof



Pisces vs Tor:
Bounded Sybil Attack Model

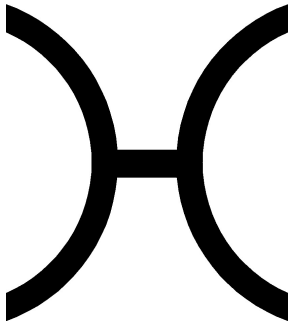




Facebook Interaction Graph with 29140 nodes

Conclusion

- Pisces anonymity system
  - Leverage social trust
  - Decentralized and scalable



- Secure random walks on unstructured topologies
  - Reciprocal neighborhood policy
  - Distributed policy enforcement