# Synchronous Batching: From Cascades to Free Routes

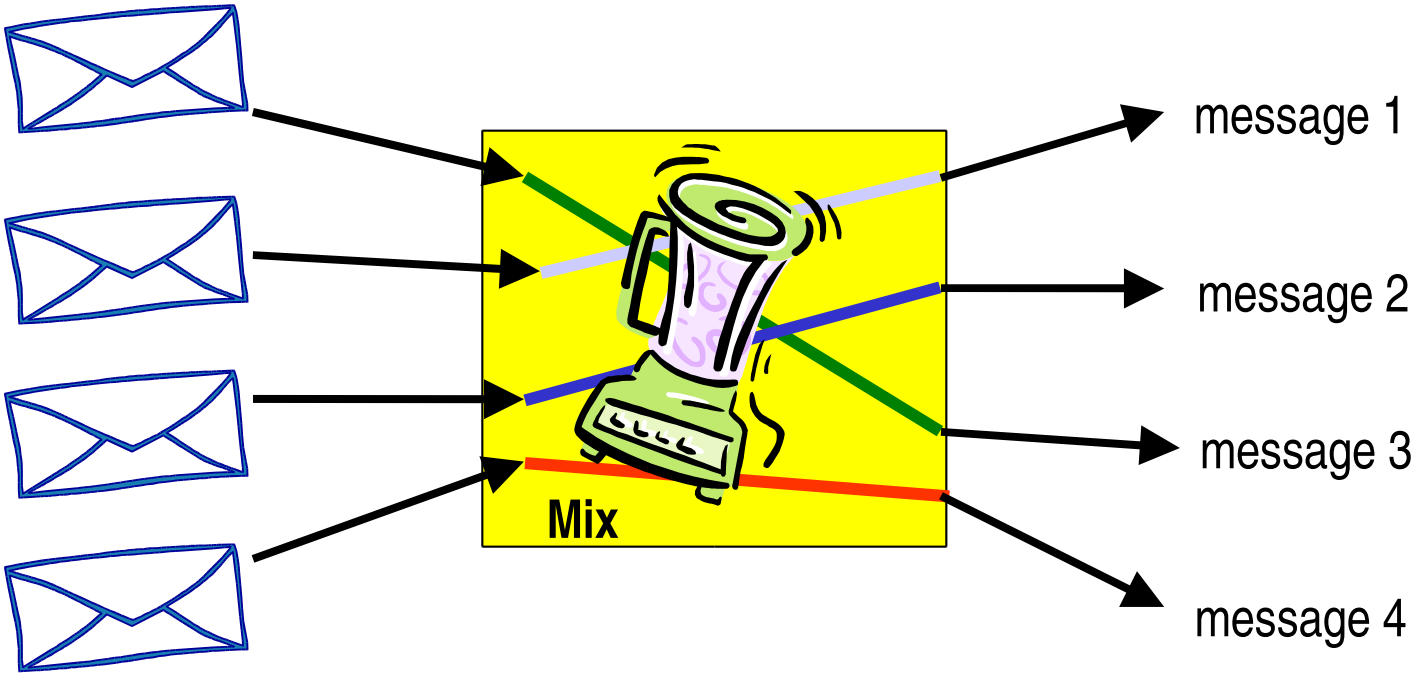
Roger Dingledine
The Free Haven Project

Vitaly Shmatikov
SRI International

Paul Syverson
Naval Research Laboratory

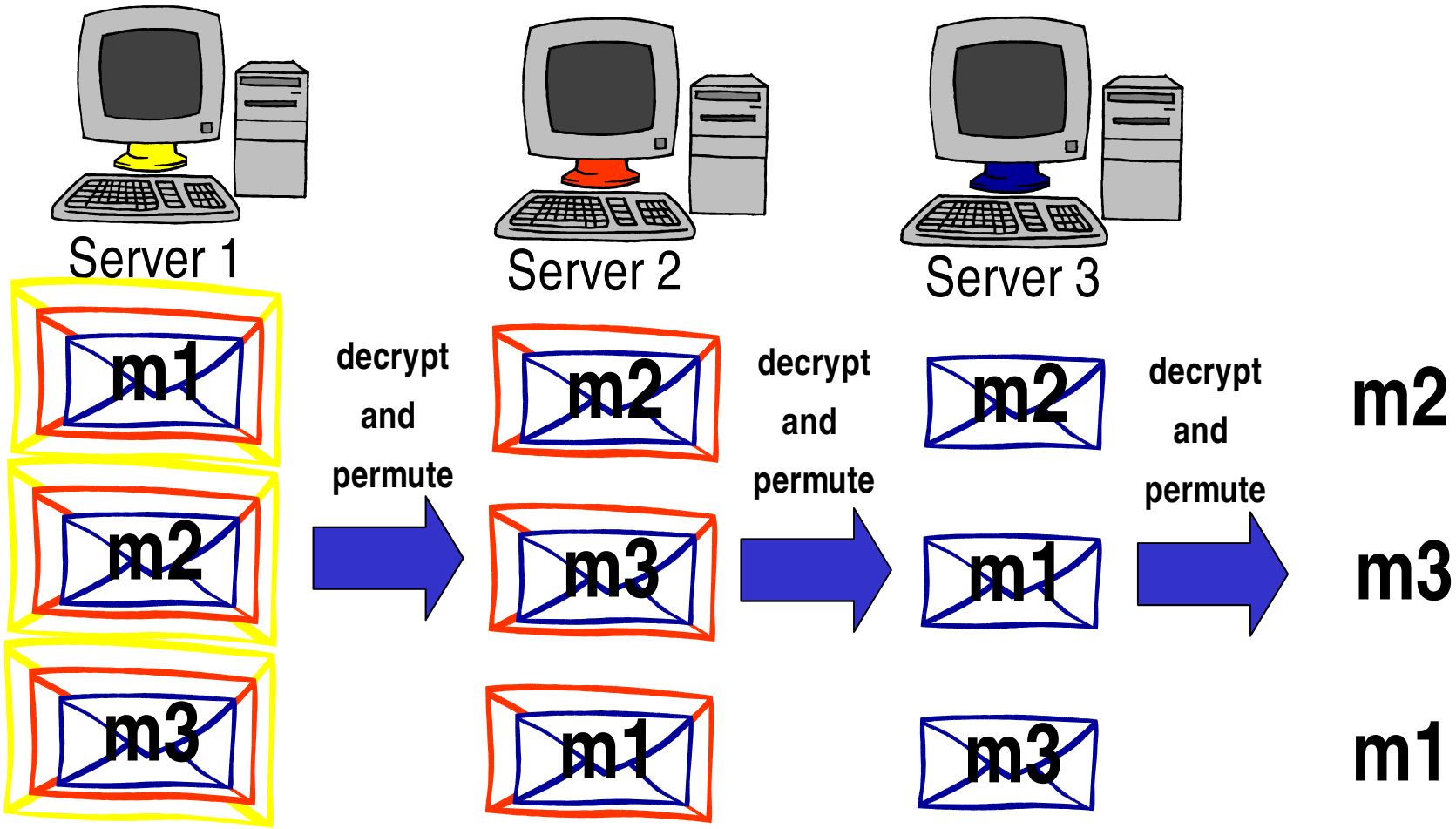
Presented at PET 2004,
May 27, 2004

# Reminder: What does a mix do?




Randomly permutes and decrypts inputs

# Basic Mix Cascade



# This paper is an update to:

## The Disadvantages of Free MIX Routes and How to Overcome Them

by Berthold, Pfitzmann, and Standke
(PET 2000)

The controversy: free routes vs cascades

Should be: asynchronous vs synchronous

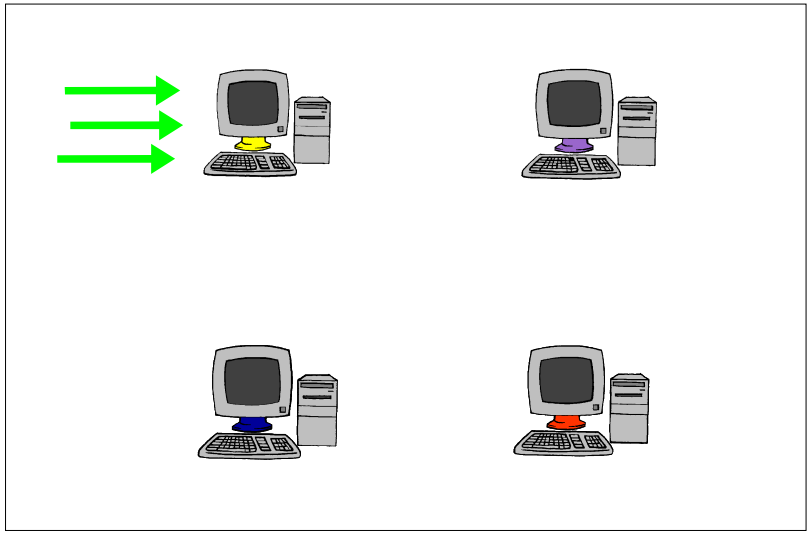
Special acknowledgement:

David Hopwood

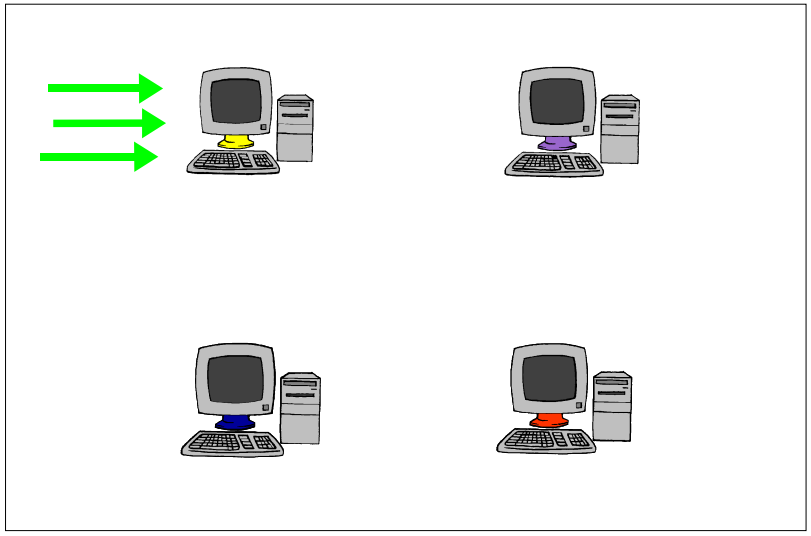
# Talk Outline

- The PET 2000 claims for cascades vs. free routes
- 3 topologies with synchronous batching
- Threat model
- Anonymity modeling methodology, results
- Synchronous batching (mixnet batching)
- Message delivery robustness
- Anonymity robustness

# Synchronous Batching



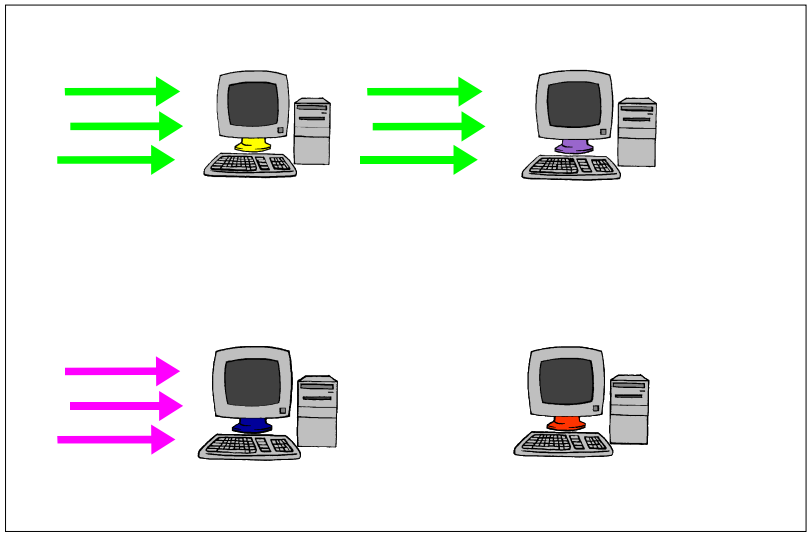
Cascade



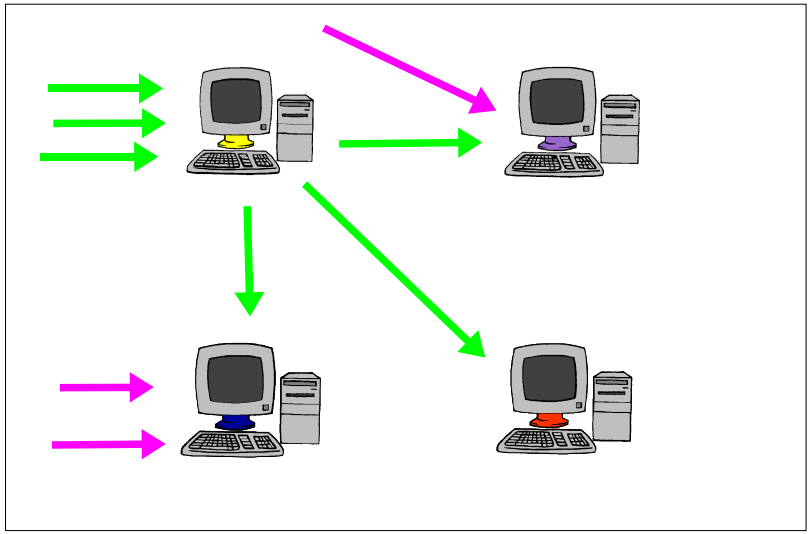
Free Route

- All messages are processed in mixnet layers

# Synchronous Batching



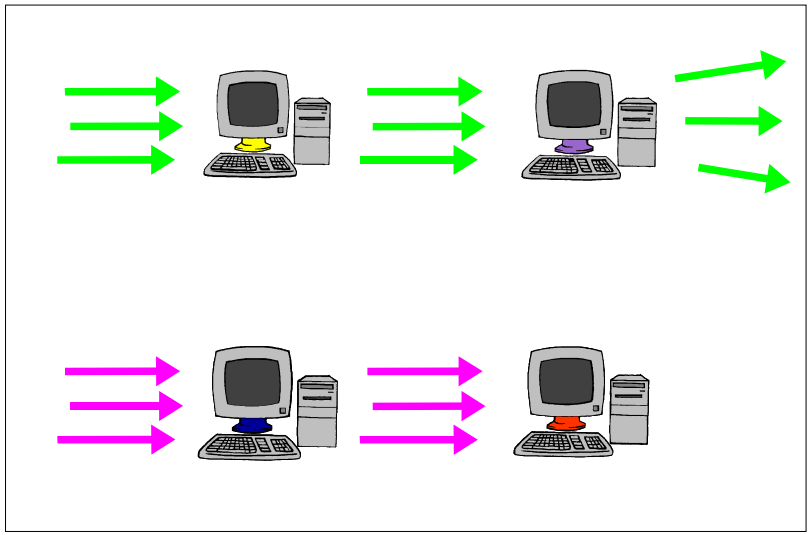
Cascade



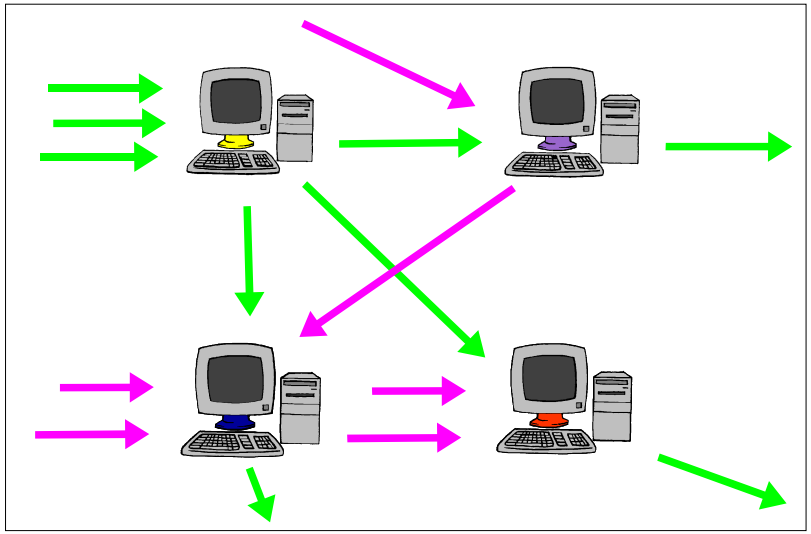
Free Route

- All messages are processed in mixnet layers

# Synchronous Batching



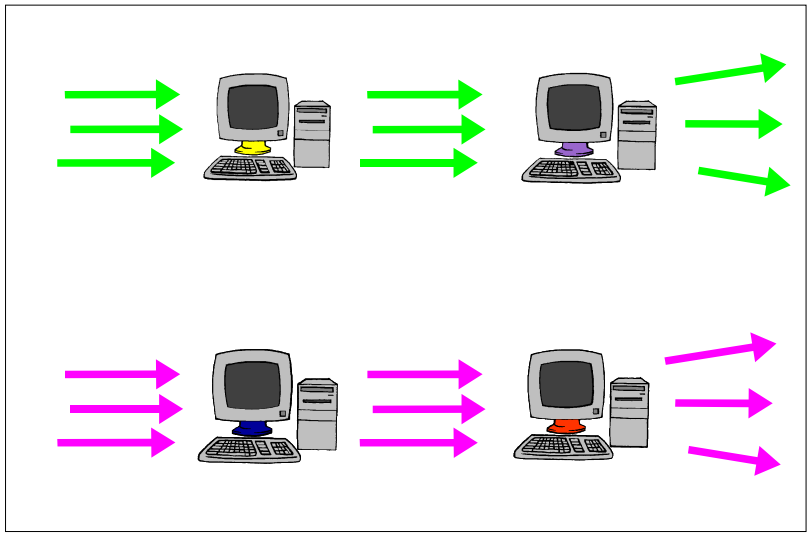
Cascade



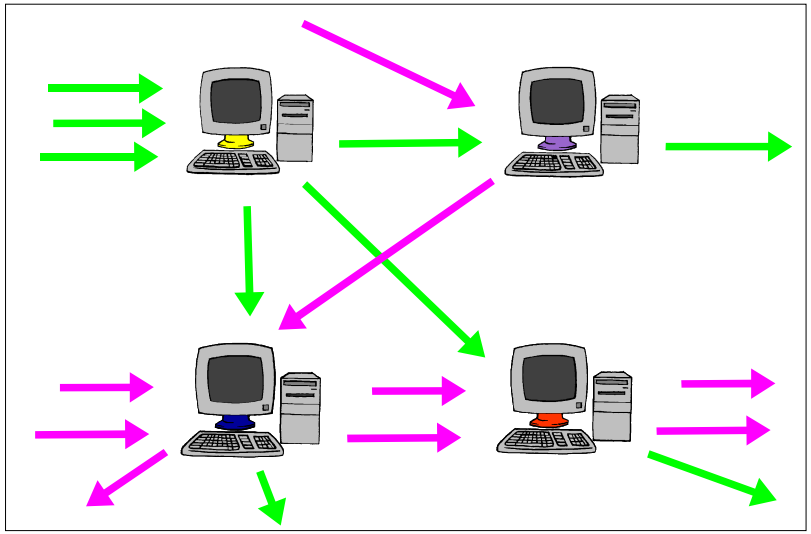
Free Route

- All messages are processed in mixnet layers

# Synchronous Batching



Cascade



Free Route

- All messages are processed in mixnet layers

# PET00 Claims: Position in Mix Route

- Assume one trustworthy mix, free routes have fixed length
- Adversary can partition messages in trustworthy mix's batch by how far along route they are
- PETs00 Claim: If only one mix is trustworthy, achievable anonymity is lower for free route than cascade
- Updated Claim: If only one mix is trustworthy, achievable anonymity is lower for asynchronous mixnet than for synchronous mixnet

# PET00 Claims: Free Route Asynchrony

- Assume one trustworthy mix, free routes have fixed length
- Anonymity set of a message in free route limited to those entering network at same time through honest nodes
- Because of asynchrony, hard to make anonymity sets the same across batches (synchronize anonymity sets)
- PETs00 Claim: Can more easily construct intersection attacks on free-route mixnets
- Updated Claim: Can more easily construct intersection attacks on asynchronous mixnets

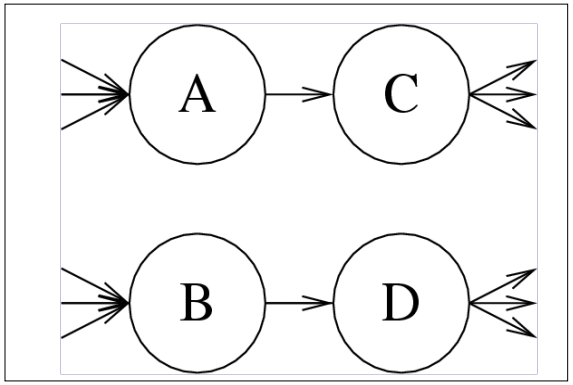
# PET00 Claims: Probability of Unobservability

- Assume one trustworthy mix, free routes have fixed length
- PETs00 Comparison: 4-node cascade with 3 bad nodes vs. 20-node free-route mixnet with 75% bad nodes
- PETs00 Claim: non-trivial chance of fully compromised paths in free-route mixnet.
- Unfair comparison: In a 20-node cascade mixnet (i.e., 5 cascades) there is also a nontrivial chance of fully compromised paths
- See analysis below

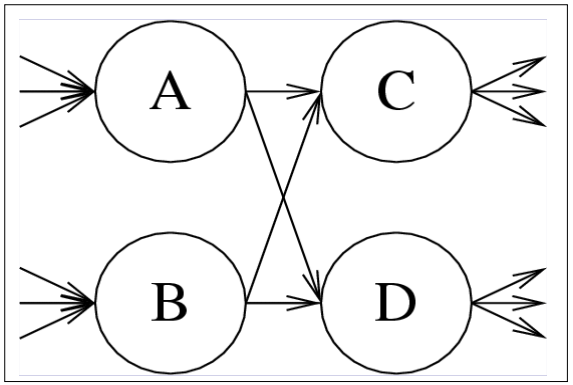
# PET00 Claims: Active Attacks

- Blending attacks: Trickle in target message while flooding with adversary message
- Countermeasures include
  - slowing attack (pool & other mixing strategies, dummy traffic)
  - preventing attack (threshold verifiable mix firing)
  - detecting &/or deterring attacker (reputation systems, ticket schemes, etc)
- These solutions apply to many topologies, not just cascades (only slowing is used in practice so far)

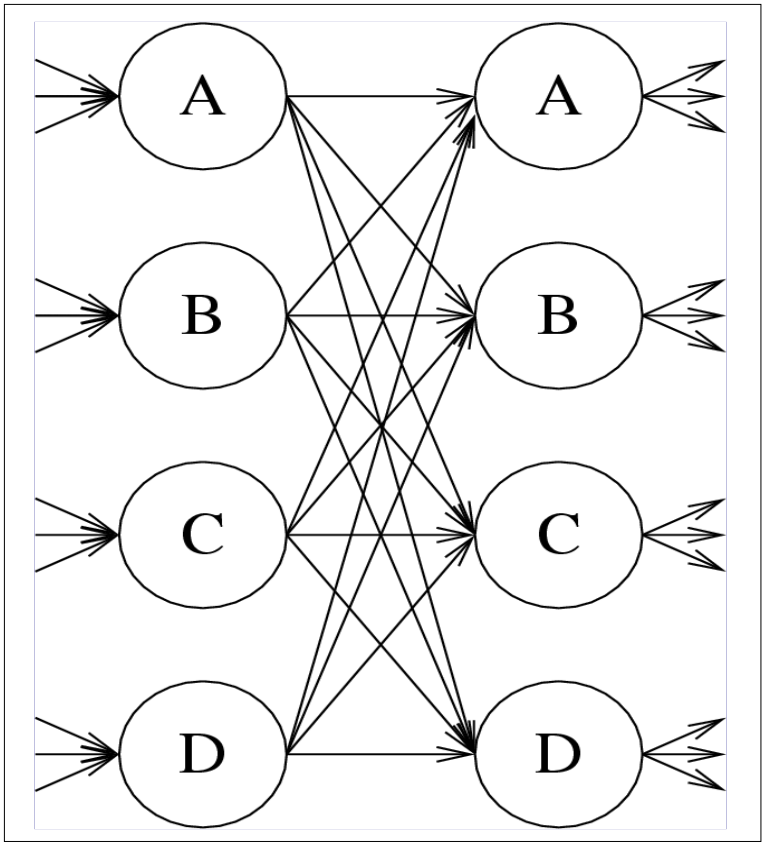
# Synchronous Mixnet Topologies for Analysis




2x2 Cascade Network




2x2 Stratified Network




4x2 Free-Route Network

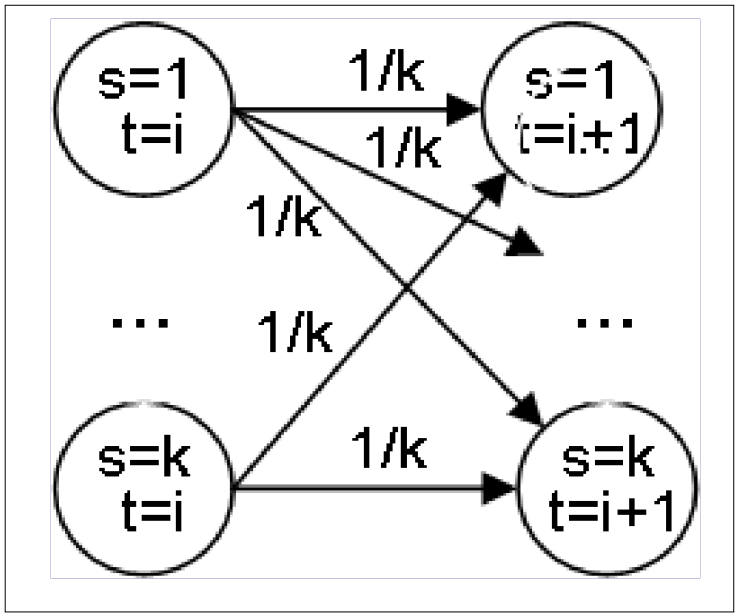
# Topology and Threat Model

- Compare three topologies: each is a 16 node network
  - 4x4 cascade
  - 4x4 stratified
  - 16x4 free-route
- Adversary compromises mix nodes at random
- Adversary is passive
- Adversary observes all messages entering / leaving mixnet
- Adversary cannot observe links between honest mix nodes
  - Simplification for modeling
  - Will argue below that significance is small

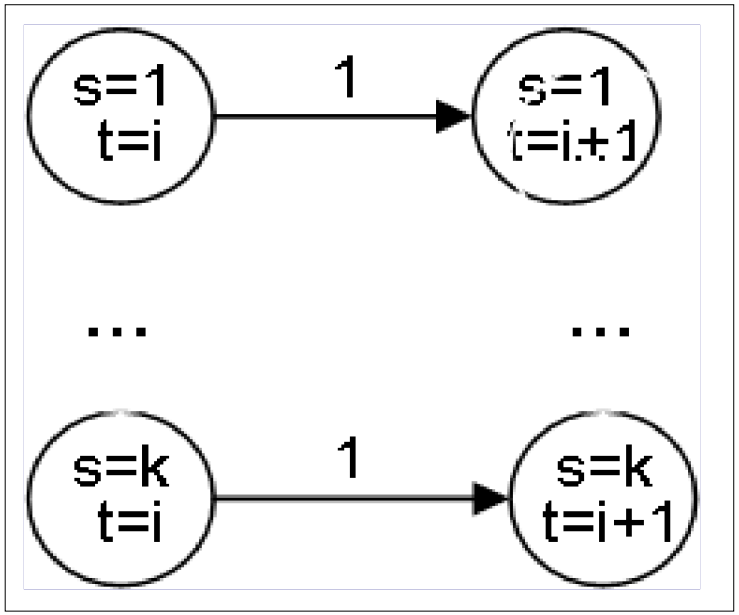
# Modeling methodology

- Mixing treated as probabilistic permutation of messages
- All N messages in mixnet batch enter in array of length N
- Good mixes permute messages, Bad mixes pass through without permuting
- Assumptions and topologies constrain choice of next mix
- Anonymity (entropy) based on probability a message exits mixnet in same position in array as entering
  - Use Markov chain to capture transitions
  - Calculate probabilities: PRISM probabilistic model checker

# A mix permutes messages



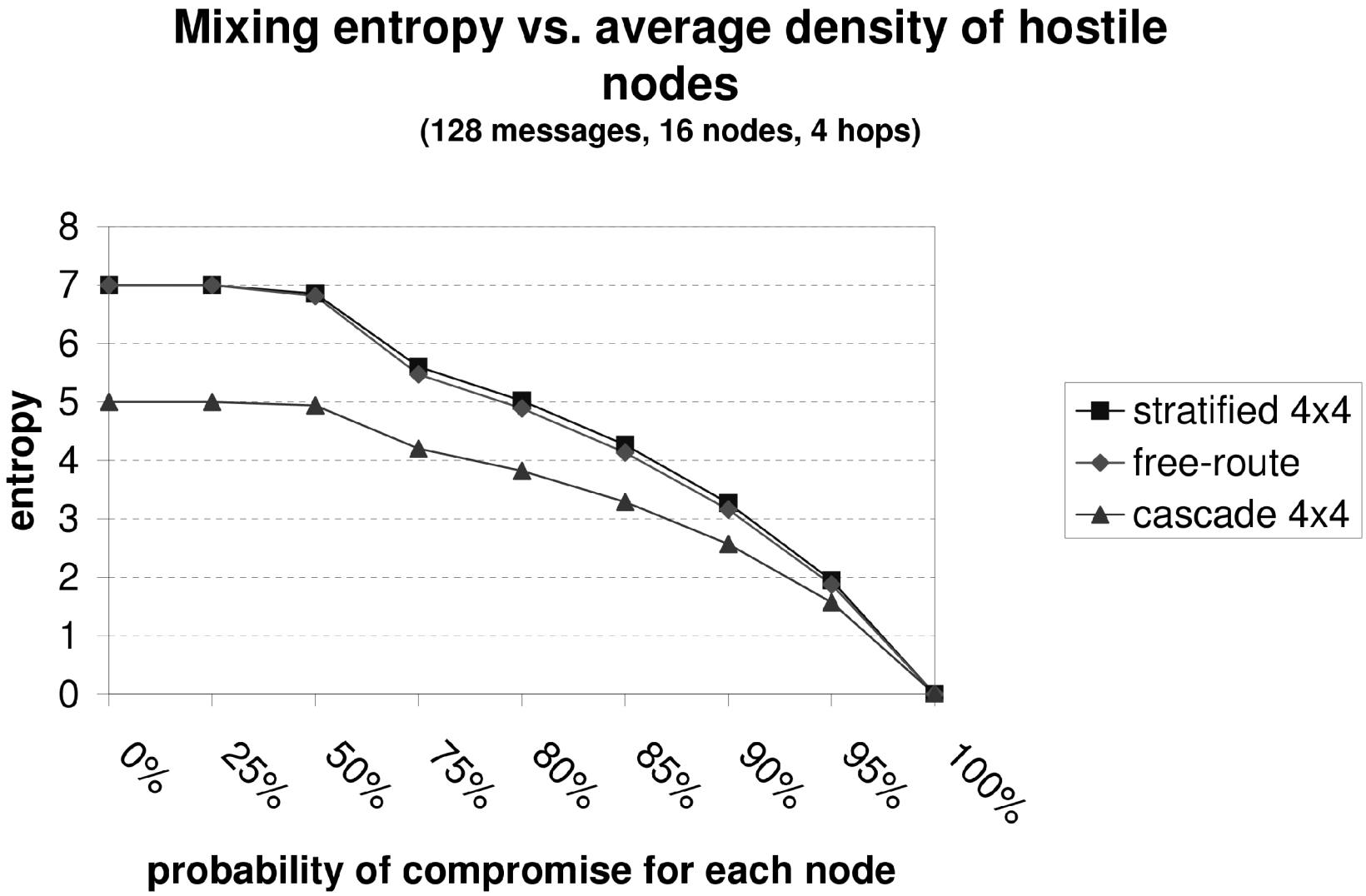

Good mix




Bad mix

- t = number of current hop
- s= position in array of k messages in mix batch

# Analysis Results



# Average Entropy!?

- Prior anonymity work calculated entropy based on specific nodes being compromised (posterior distributions)
- We calculate anonymity based on fixed probability any node might be compromised (prior distributions)
- Effectively the average of possible node compromise

# Why not just one cascade?

- Bandwidth of a single node is insufficient?
- A single cascade may not include as many jurisdictions as a user wants?
- A single cascade is not very robust (to network attacks, or nature).

# Are all links actually balanced?

For $m$ message in $u$ buckets (nodes in layer) what are chances of less than $p$ messages in a bucket?

Example:

m = 128, u = 4 (cascade or stratified) $\Rightarrow$

chances of less than 16 messages (vs. 32 expected) is .0006

m = 128, u = 16 (free-route) $\Rightarrow$

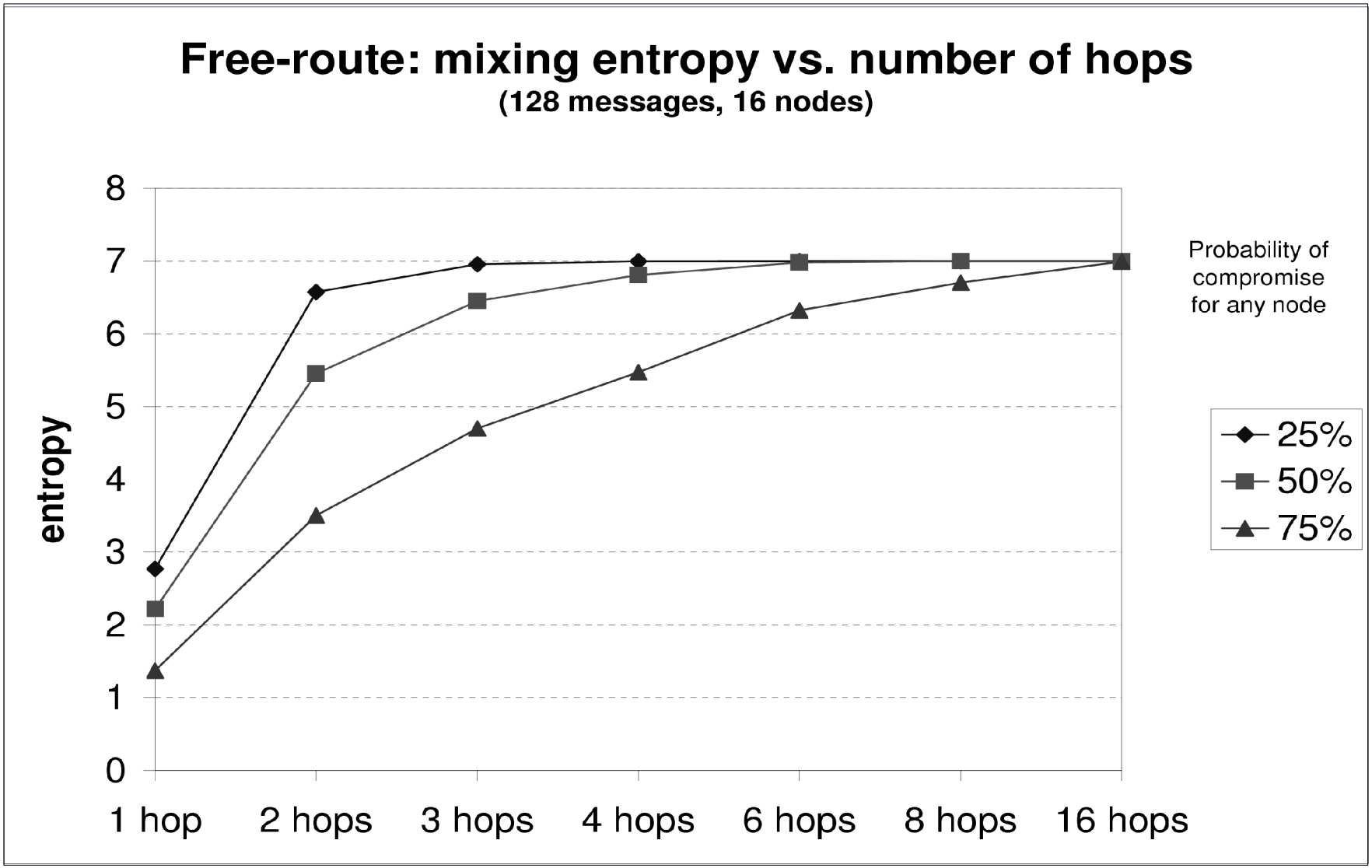
chances of less than 16 messages is .48

m = 480, u = 16 (free-route) $\Rightarrow$

chances of less than 16 messages is .01

(Mixmaster network currently gets over 1000 msg/hr)

# Anonymity vs. Hops



# Robustness of Message Delivery

| | Topology | 1 crash | 2 crash | 3 crash | 4 crash |
|---|---|---|---|---|---|
| Worst possible adversary distribution | 16x16 free | 36 | 12 | 04 | 01 |
| | 4x4 cascade | 75 | 50 | 25 | 00 |
| | 4x4 stratif. | 75 | 50 | 25 | 00 |
| | 16x4 free | 77 | 59 | 44 | 32 |
| Best possible adversary distribution | 16x16 free | 36 | 12 | 04 | 01 |
| | 4x4 cascade | 75 | 75 | 75 | 75 |
| | 4x4 stratif. | 75 | 56 | 42 | 32 |
| | 16x4 free | 77 | 59 | 44 | 32 |
| Expected percentage: rand. adversary dist. | 16x16 free | 36 | 12 | 04 | 01 |
| | 4x4 cascade | 75 | 55 | 39 | 27 |
| | 4x4 stratif. | 75 | 55 | 39 | 27 |
| | 16x4 free | 77 | 59 | 44 | 32 |

Table 1: Percent of messages delivered vs number of crashed nodes

# Robustness of Anonymity

- Consider adversary that crashes nodes to reduce entropy
- No effect on cascades: all messages or none are delivered
- Stratified only affected by entry node failure
  - 1 fail: entropy reduces by .42
  - 2 fail: entropy drops by 1
  - 3 fail: entropy drops by 2
  - all fail: no information
- At worst stratified provides same entropy as cascades

# Robustness of Anonymity

- Free Route is complicated: killing a node could block target messages later
- Assume very lucky adversary owning 4 nodes
  - Crashes all nodes without affecting target message at any layer
  - Remaining messages are .32 of original batch
- This is still better than the .25 of original batch a mix cascade processes

# Synchronous Free-routes vs Asynchronous Free-routes

- Better protection against partitioning attacks
- No need for replay detection: just mark each message with its batch
- Easier to verify if messages are delivered
- But: cannot use any pooling strategy
  - More vulnerable to longterm statistical disclosure attack?
- Less robust against transient failure
  - In asynchronous design, a late message still arrives

# Summary

- Previously, cascade topology was thought necessary to guard against certain powerful adversaries
- We have shown that other synchronous mixnet designs generally do as well or better than cascades
  - For anonymity with a passive adversary
  - For message delivery
  - For anonymity robustness with an active adversary