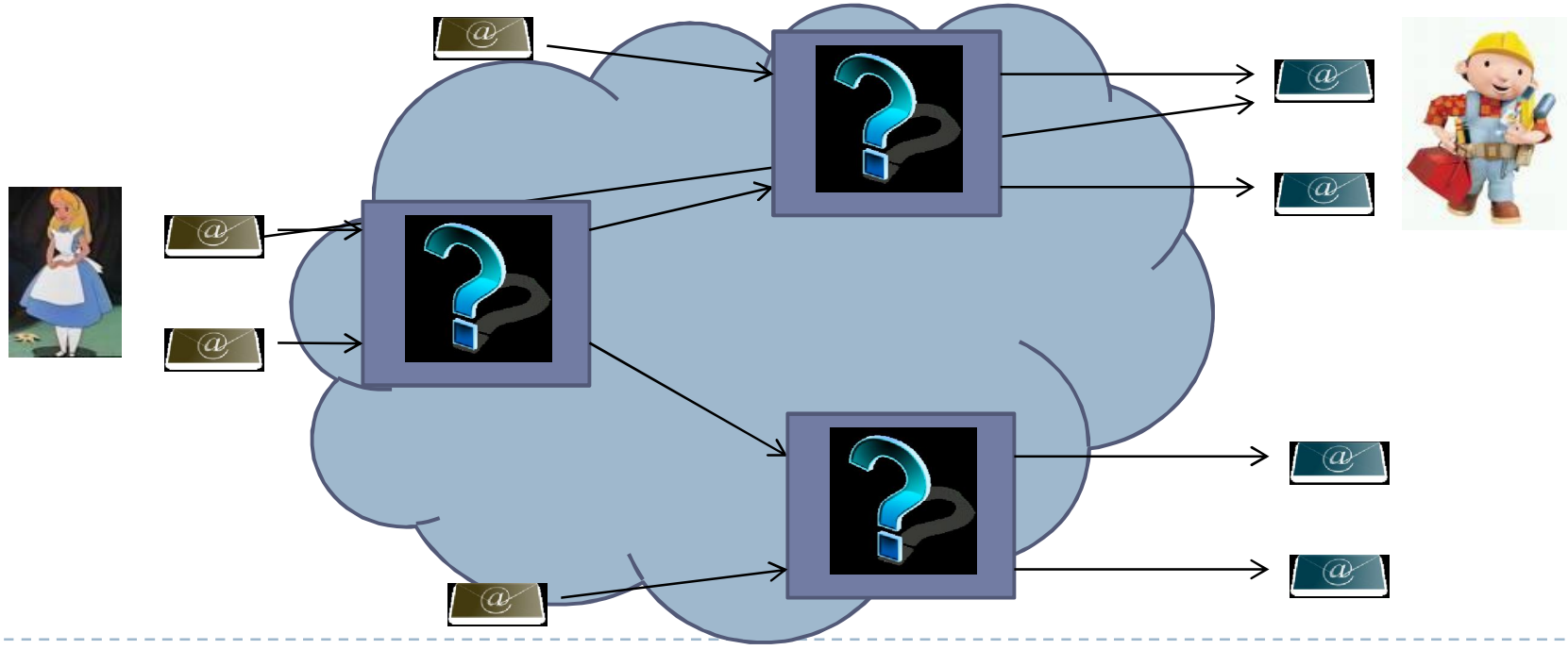
# Bayesian Inference and Traffic Analysis

**Carmela Troncoso**
George Danezis

September-November 2008
Microsoft Research Cambridge/ KU Leuven(COSIC)

# Anonymous Communications

- "Tell me who your friends are..." =>Anonymous communications to hide communication partners
- High latency systems (e.g. anonymous remailers) use mixes [Chaum 81]: hide input/output relationship



# Anonymous Communications

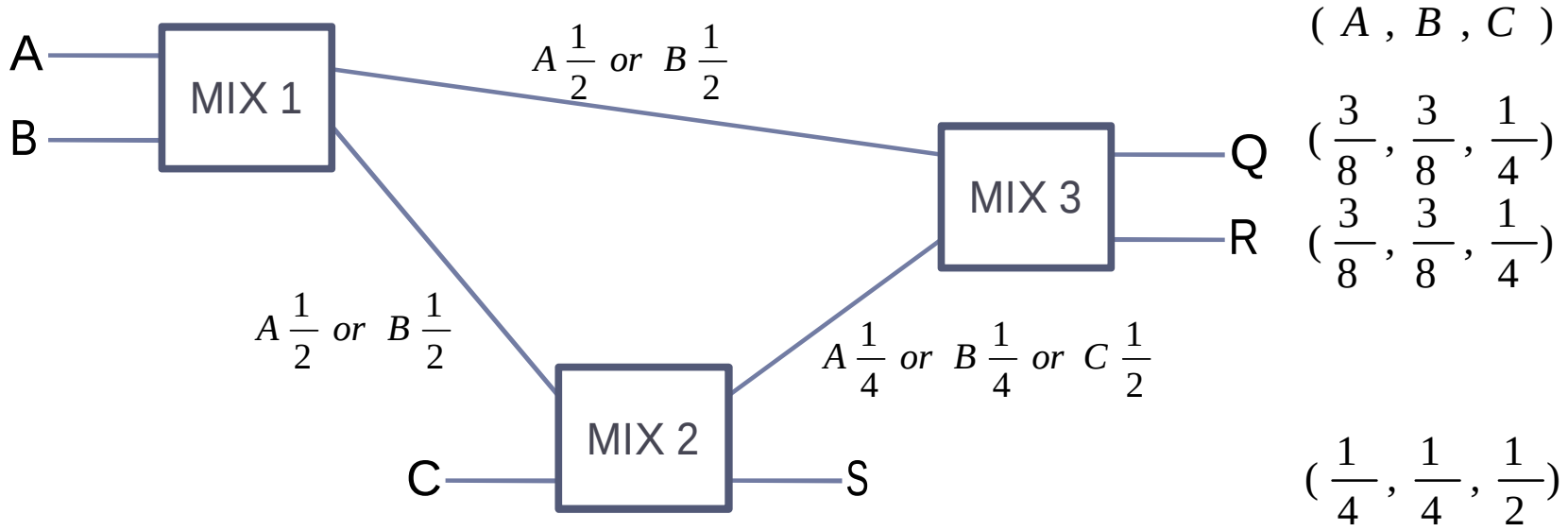
- Attacks to mix networks
  - Restricted routes [Dan03]
  - Bridging and Fingerprinting [DanSyv08]

  - Social information:
    - Disclosure Attack [Kes03],
    - Statistical Disclosure Attack [Dan03],
    - Perfect Matching Disclosure Attacks [Tron08]

- Heuristics and specific models

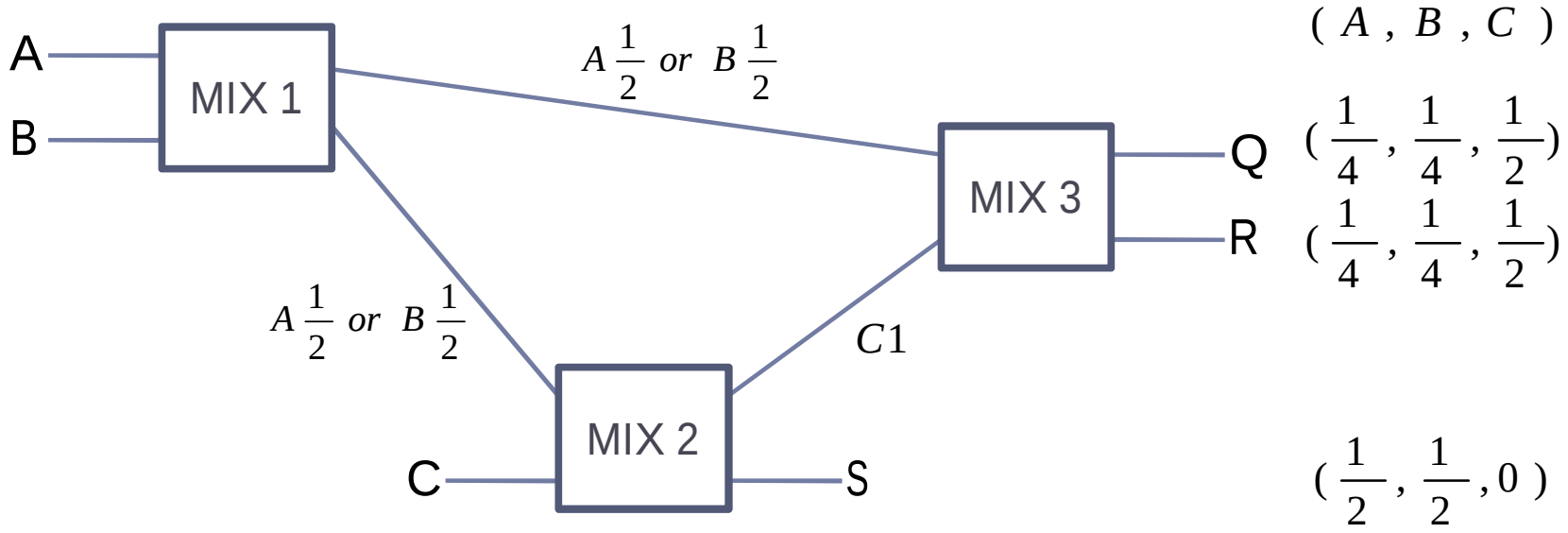
# Mix networks and traffic analysis

- Determine probability distributions input-output



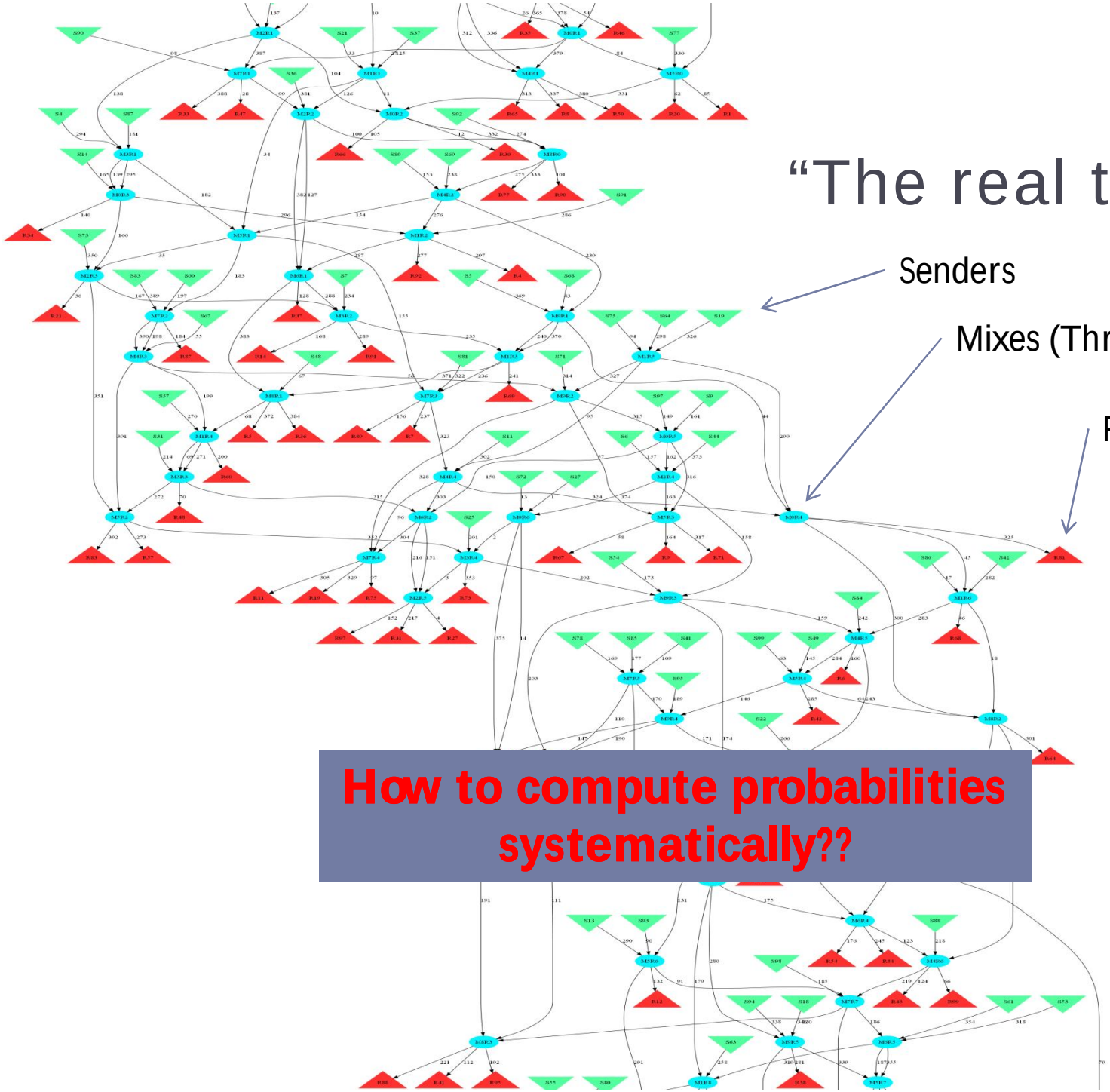
# Mix networks and traffic analysis

- Constraints,e.g.length=2




Non trivial given observation!!

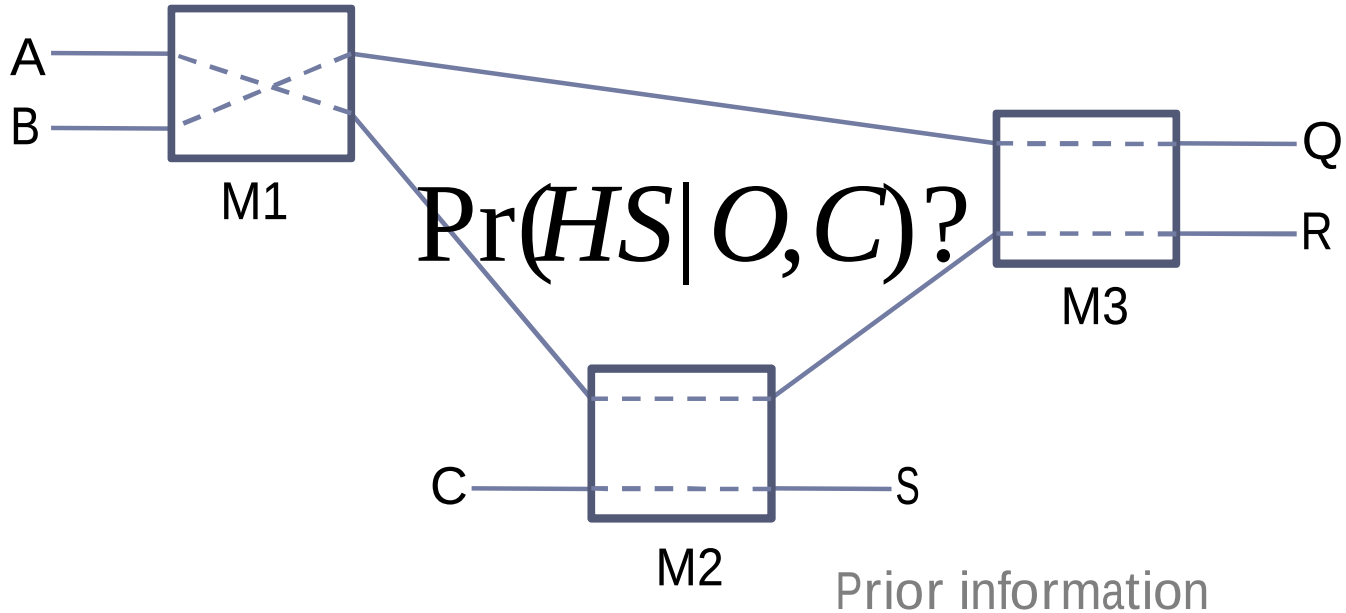
# “The real thing”




**How to compute probabilities systematically??**

# Mix networks and traffic analysis

- Find *"hidden state"* of the mixes



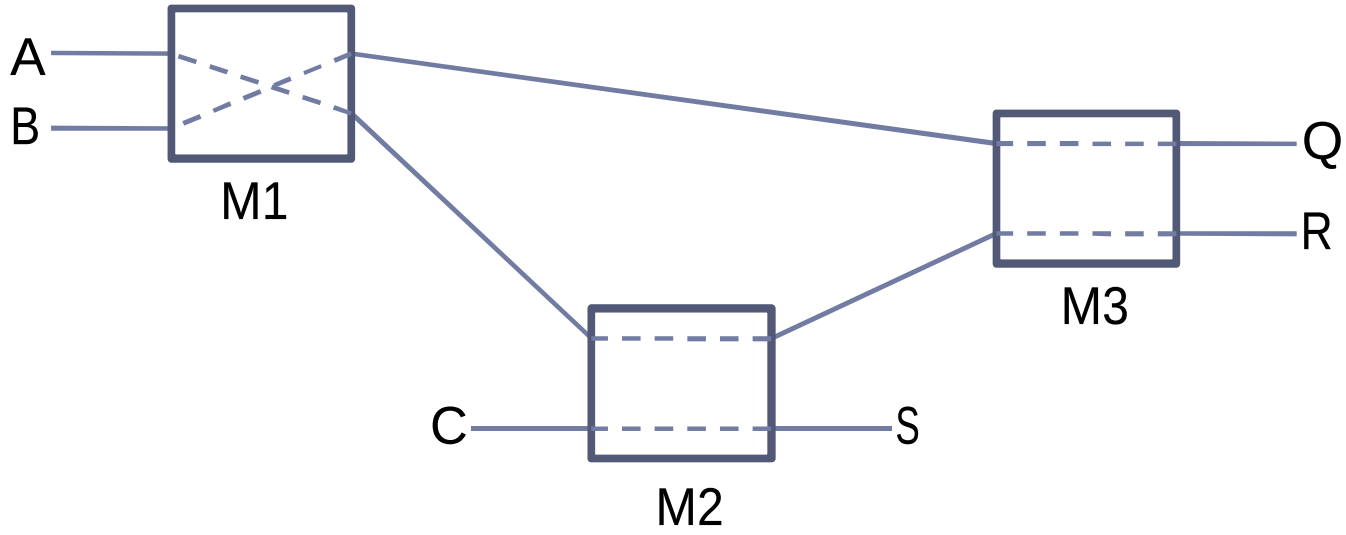

Prior information

$$\Pr(HS \mid O,C) = \frac{\Pr(O \mid HS,C)\cdot \Pr(HS \mid C)}{\sum_{HS} \Pr(HS,O \mid C)} = \frac{\Pr(O \mid HS,C)\cdot K}{Z}$$

Too large to enumerate!!

# Mix networks and traffic analysis

- *"hidden state"+ Observation = Paths*

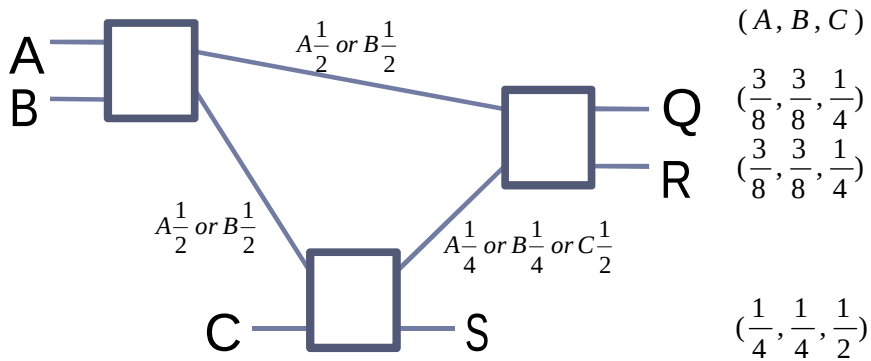



$P_1 \rightarrow$ A — M1 — M2 — M3 — R
$P_2 \rightarrow$ B — M1 — M3 — Q
$P_3 \rightarrow$ C — M2 — S

$$\Pr(HS \mid O, C) = \frac{\Pr(O \mid HS, C) \cdot K}{Z} = \frac{\Pr(Paths \mid C)}{Z}$$

# Bayesian Inference

- Actually… we want marginal probabilities




$$\Pr(A \to Q \mid HS, O, C) = \frac{\sum_{HS} I_{A \to Q}(HS_j)}{j}$$

- But… we cannot obtain them directly

# Bayesian Inference - sampling

- If we obtain samples

$$HS_1, HS_2, HS_3, HS_4, \ldots, HS_j \sim \Pr(HS \mid O, C)$$

$(A \rightarrow Q)?$ 0 1 0 1 … 1

$$\Pr(A \rightarrow Q \mid HS, O, C) = \frac{\sum_{HS} I_{A \rightarrow Q}(HS_j)}{j}$$

- Markov Chain Monte Carlo Methods
  - Metropolis Hastings algorithm

$$\Pr(HS \mid O, C) = \frac{\Pr(Paths \mid C)}{Z}$$

How does *Pr(Paths|C)* look like?

# Probabilistic model – Basic Constraints

- Users decide independently

$$\Pr(Paths \mid C) = \prod_x \Pr(P_x \mid C)$$

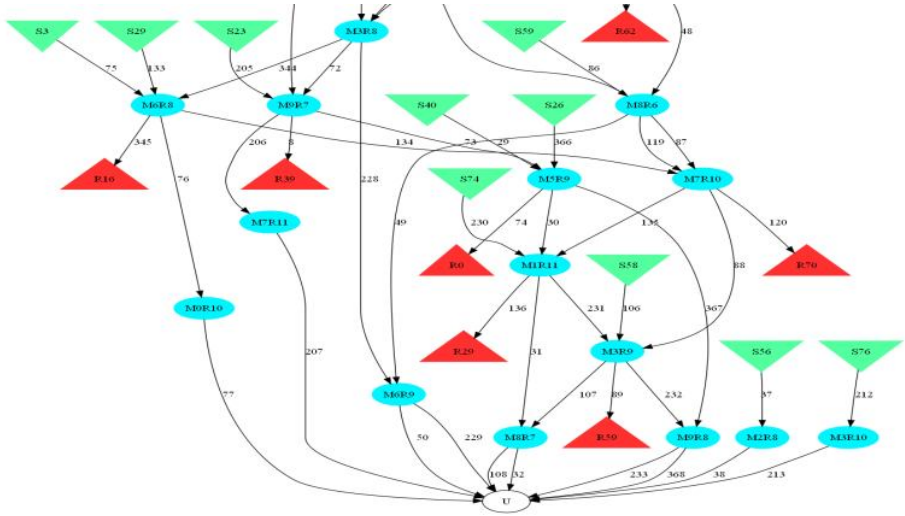
- Length restrictions $\Pr(L = l \mid C)$ with any distribution
  - e.g.uniform ($L_{min}$, $L_{max}$) $\Pr(L = l \mid C) = \frac{1}{L_{\max} - L_{\min}}$

- Node choice restrictions
  - Choose l out of the $N_{mix}$ node available $\Pr(M_x \mid L = l, C) = \frac{1}{P(N_{mix}, l)}$
  - Choose a set $I_{set}(M_x)$

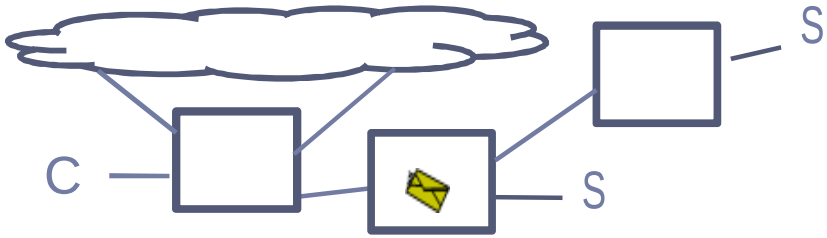
$$\Pr(P_x \mid C) = \Pr(L = l \mid C) \cdot \Pr(M_x \mid L = l, C) \cdot I_{set}(M_x)$$

# Probabilistic model – Basic Constraints

- Unknown destinations



$$L_{\max} = 3$$




$$\Pr(P_x \mid C) = \left[ \sum_{l=L_{obs}}^{L_{\max}} \Pr(L = l \mid C) \cdot \Pr(M_x \mid L = l, C) \cdot I_{set}(M_x) \right]$$

# Probabilistic model – More Constraints

- Bridging
  - Known nodes $I_{bridging}\ (M_x)$
- Non-compliant clients (with probability $p_{\overline{cp}}$)
  - Do not respect length restrictions $(L_{\min,\overline{cp}}, L_{\max,\overline{cp}})$
  - Choose l out of the $N_{mix}$ node available,allow repetitions

$$\Pr(M_x \mid L = l, C, I_{\overline{cp}}(Path)) = \frac{1}{P_r(N_{mix}, l)}$$

$$\Pr(Paths \mid C) = \prod_x \Pr(P_x \mid C)$$

$$\Pr(Paths \mid C) = \left[\prod_{i \in P_{\overline{cp}}} p_{\overline{cp}} \Pr(P_i \mid C, I_{\overline{cp}}(P_i))\right] \cdot \left[\prod_{j \in P_{cp}} (1 - p_{\overline{cp}}) \Pr(P_j \mid C)\right]$$

# Probabilistic model – More constraints

- Social network information
  - Assuming we know sending profiles $\Pr(\text{Sen}_x \rightarrow \text{Rec}_x)$

$$\Pr(P_x \mid C) = \Pr(L = l \mid C) \cdot \Pr(M_x \mid L = l, C) \cdot I_{set}(M_x) \cdot \Pr(\text{Sen}_x \rightarrow \text{Rec}_x)$$

- Other constraints
  - Unknown origin
  - Dummies
  - Other mixing strategies
  - ….

# Markov Chain Monte Carlo

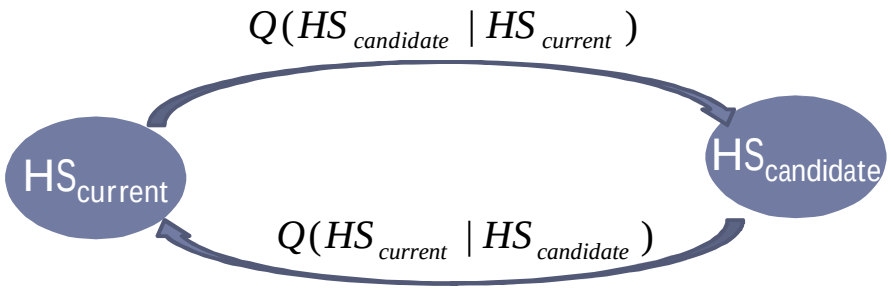
- Sample from a distribution difficult to sample from directly

$$\Pr(HS \mid O, C) = \frac{\Pr(O \mid HS, C) \cdot \Pr(HS \mid C)}{\sum_{HS} \Pr(HS, O \mid C)} = \frac{\Pr(O \mid HS, C) \cdot K}{Z} = \frac{\Pr(Paths \mid C)}{Z}$$

- 3 Key advantages:
  - Requires generative model (we know how to compute it!)
  - Good estimation of errors
    - Not false positives and negatives
  - Systematic

# Metropolis Hastings Algorithm

- Constructs a Markov Chain with stationary distribution $\Pr(HS \mid O, C)$
  - Current state $\xrightarrow{Q}$ Candidate state




1. Compute $\alpha = \dfrac{\Pr(HS_{candidate})Q(HS_{candidate} \mid HS_{current})}{\Pr(HS_{current})Q(HS_{current} \mid HS_{candidate})}$
2. If $\alpha \geq 1$

   $HS_{current} = HS_{candidate}$

   else $u \sim U(0,1)$

   if $u \leq \alpha$

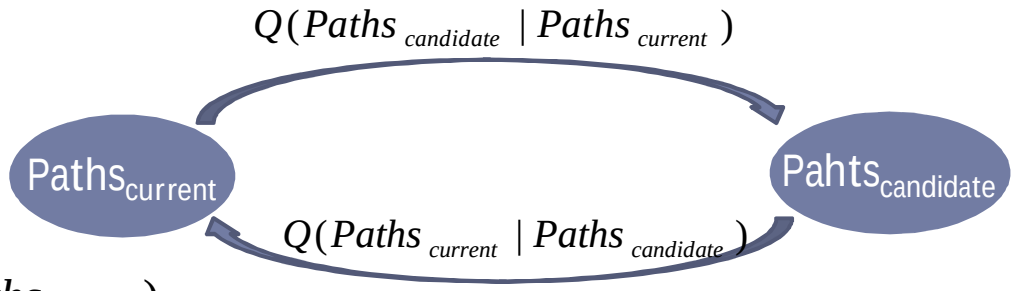
   $HS_{current} = HS_{candidate}$

   else

   $HS_{current} = HS_{current}$

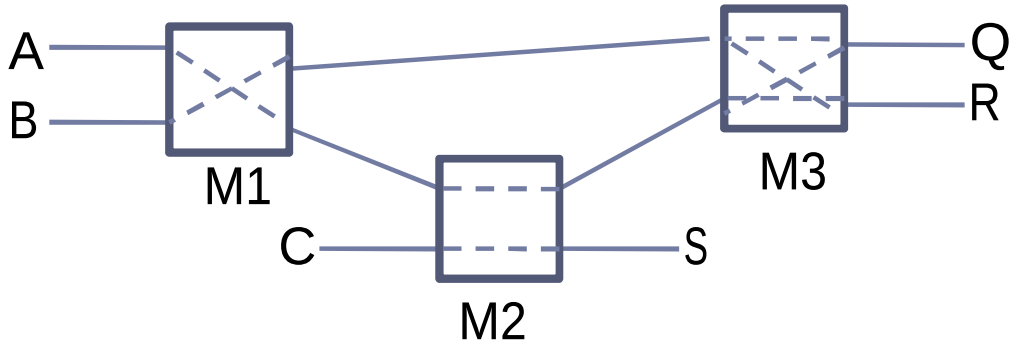
# Our sampler: Q transition

$$\Pr(HS \mid O, C) = \frac{\Pr(Paths \mid C)}{Z}$$




$$\alpha = \frac{\Pr(Paths_{candidate})Q(Paths_{candidate} \mid Paths_{current})}{\Pr(Paths_{current})Q(Paths_{current} \mid Paths_{candidate})}$$

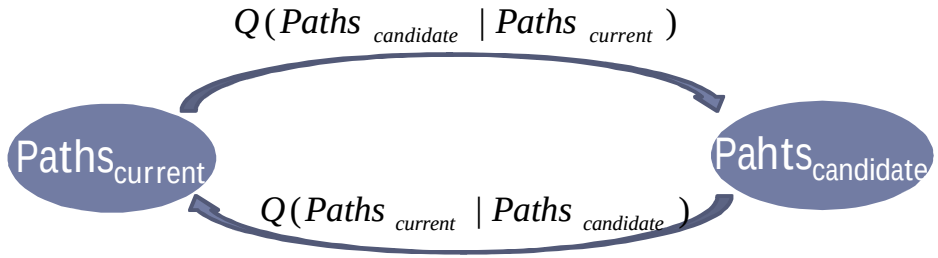
- Transition Q: swap operation

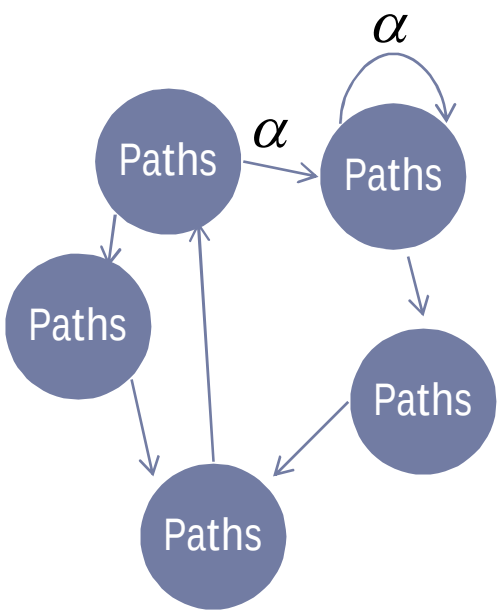



  - More complicated transitions for non-compliant clients

# Iterations

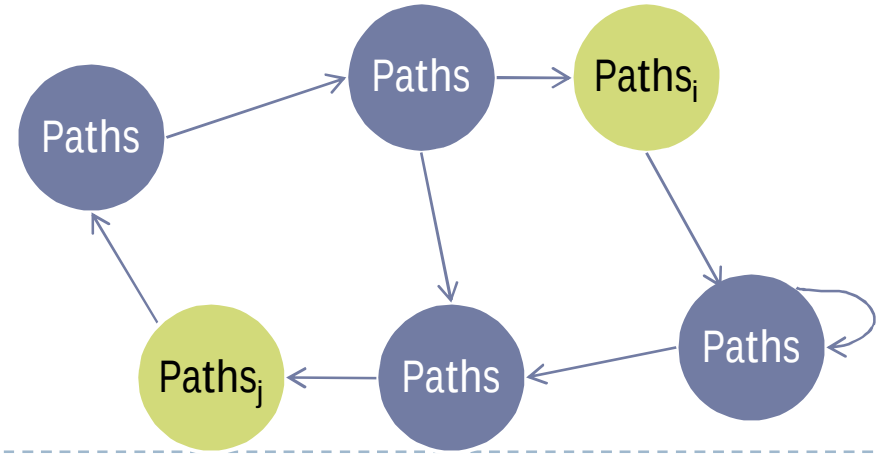
$$\Pr(HS \mid O, C) = \frac{\Pr(Paths \mid C)}{Z}$$



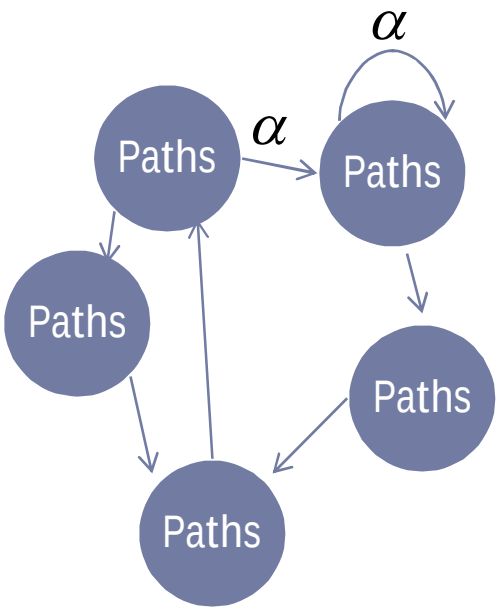




- Consecutive samples dependant
  - Sufficiently separated

$$\Pr(Paths_i \mid Paths_j) = \Pr(Paths_i)$$



# Error estimation




$$(A \rightarrow Q)?\quad \overset{P_1}{\downarrow}\ \overset{P_2}{\downarrow}\ \overset{P_3}{\downarrow}\ \overset{P_4}{\downarrow}\quad 1\ \ 0\ \ 1\ \ 0 \longrightarrow \Pr(A \rightarrow Q) = \frac{\sum I_{A \rightarrow Q}}{j}$$

- Error estimation
  - Bernouilli distribution

$$\Pr[Paths_1, Paths_2, Paths_3, \ldots \mid \Pr(A \rightarrow Q)]$$

  - Prior Beta(1,1) ~ uniform

$$\Pr[\Pr(A \rightarrow Q) \mid Paths_1, Paths_2, Paths_3, \ldots]$$

$$\Pr(A \rightarrow Q) \sim Beta\left(\sum_{Paths} I_{A \rightarrow Q}(Path_i) + 1, \sum_{Paths} I_{\neg A \rightarrow Q}(Path_i) + 1\right)$$

  - Confidence intervals

# Evaluation

1. Create an instance of a network
2. Run the sampler
3. Choose a target sender and a receiver
4. Estimate probability

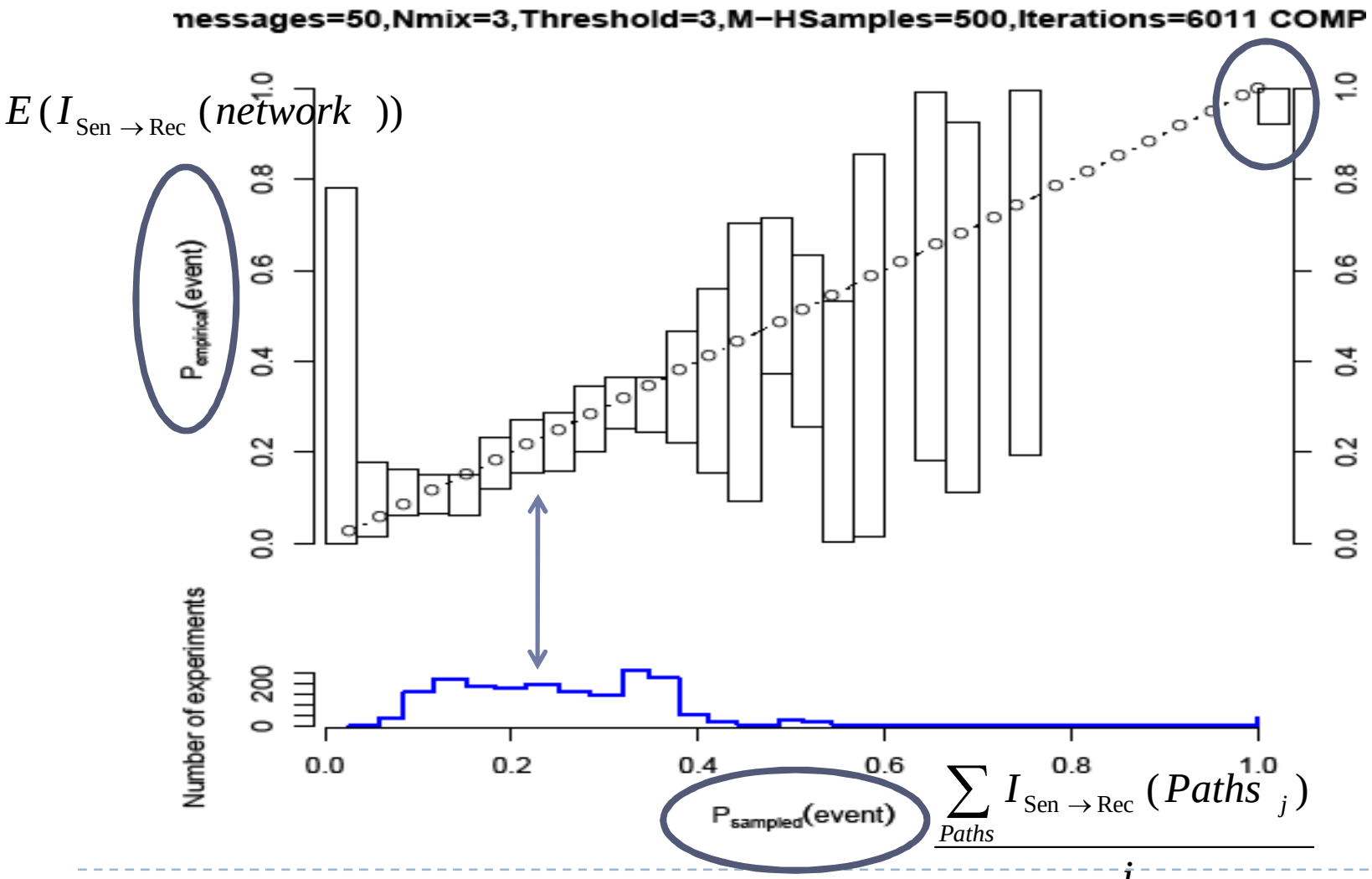
$$\Pr(\text{Sen} \rightarrow \text{Rec}) = \frac{\sum_{Paths} I_{\text{Sen} \rightarrow \text{Rec}}(Paths_j)}{j}$$

5. Check if actually Sen chose Rec as receiver $I_{\text{Sen} \rightarrow \text{Rec}}(network)$
6. Choose new network and go to 2

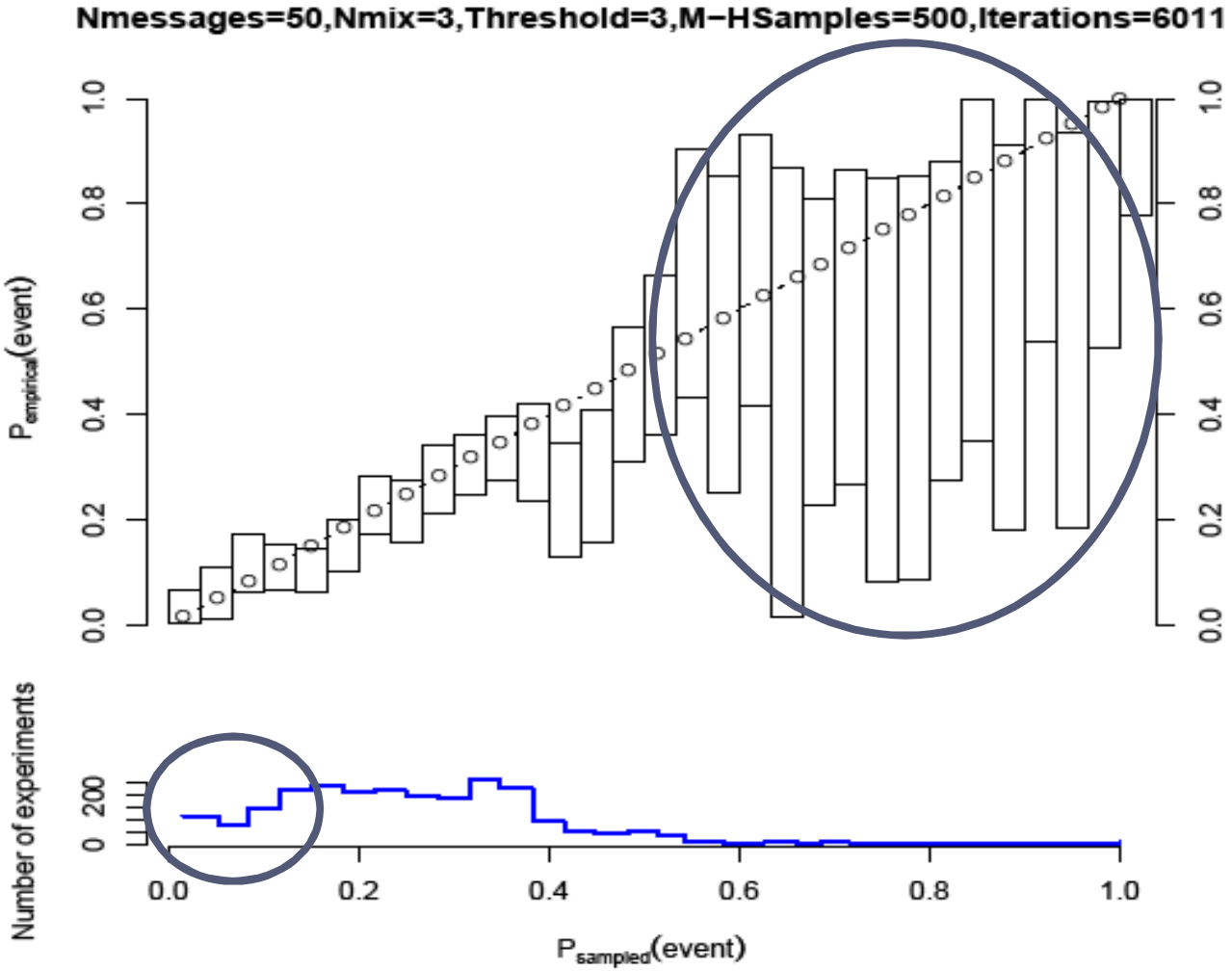
Events should happen with the estimated probability

$$\Pr(\text{Sen} \rightarrow \text{Rec}) = \frac{\sum_{Paths} I_{\text{Sen} \rightarrow \text{Rec}}(Paths_j)}{j} = E(I_{\text{Sen} \rightarrow \text{Rec}}(network))$$

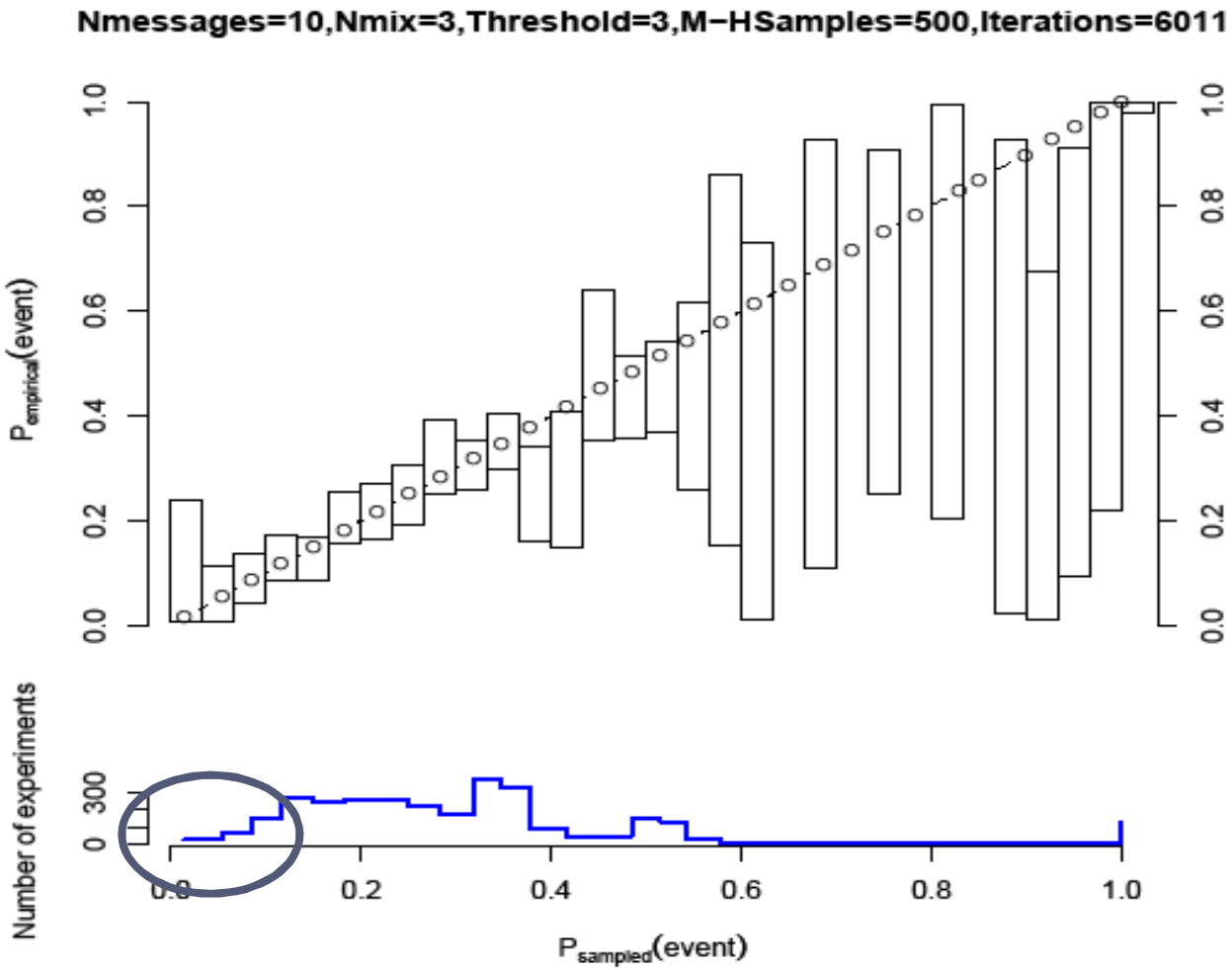
# Results – compliant clients



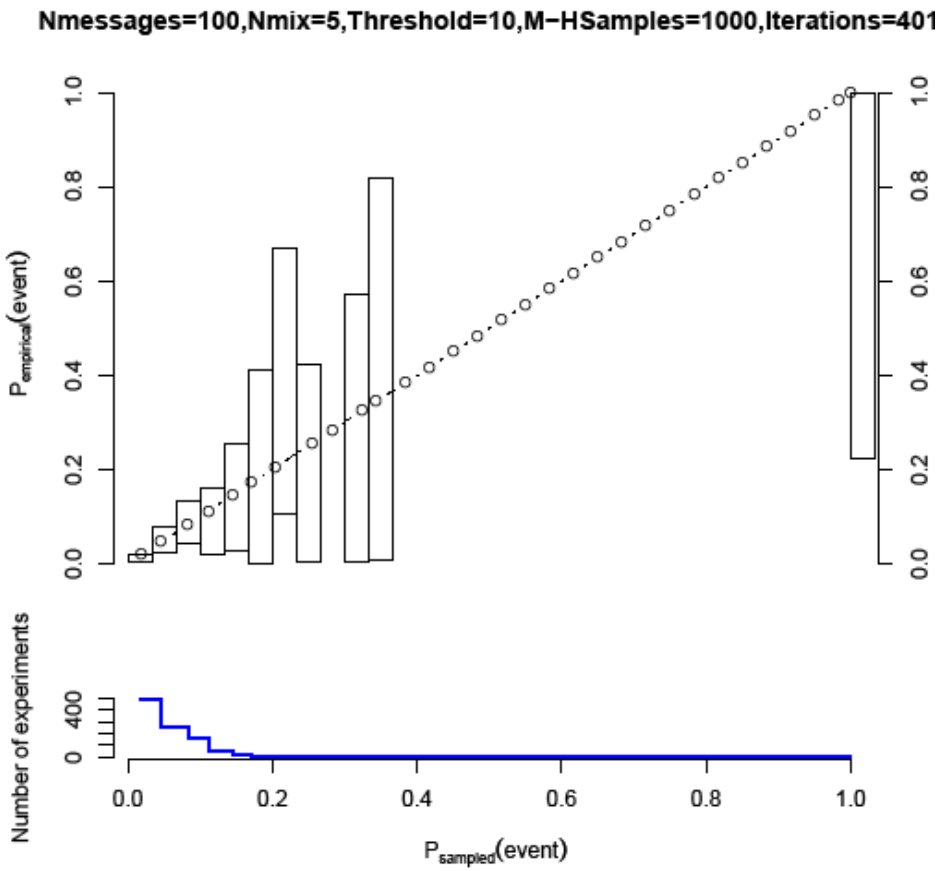
# Results – 50 messages

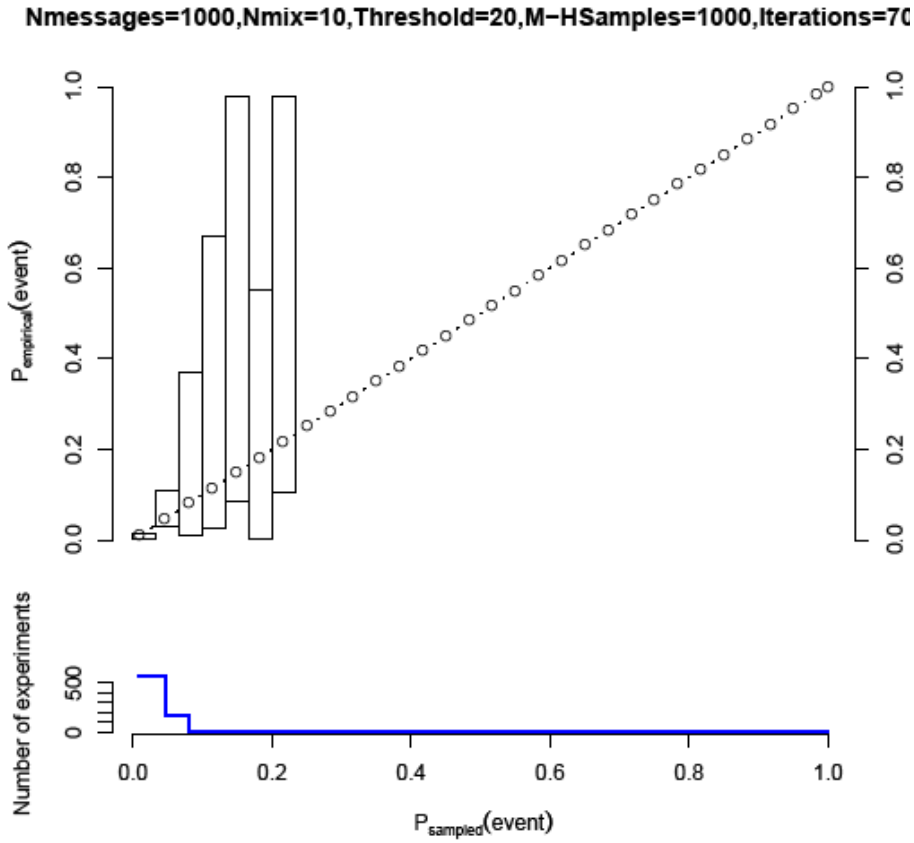


# Results – 10 messages



# Results – big networks



# Performance – RAM usage

| Nmix | t | Nmsg | Samples | RAM(Mb) |
|---|---|---|---|---|
| 3 | 3 | 10 | 500 | 16 |
| 3 | 3 | 50 | 500 | 18 |
| 5 | 10 | 100 | 500 | 19 |
| 10 | 20 | 1 000 | 1 000 | 24 |
| 10 | 20 | 10 000 | 1 000 | 125 |

- Size of network and population
- Results are kept in memory during simulation
- Number samples collected increases

# Performance – Running time

| Nmix | t | Nmsg | iter | Full analysis (min) | One sample(ms) |
|---|---|---|---|---|---|
| 3 | 3 | 10 | 6011 | 2.33 | 267.68 |
| 3 | 3 | 50 | 6011 | 2.55 | 306.00 |
| 5 | 10 | 100 | 4011 | 1.58 | 190.35 |
| 10 | 20 | 1 000 | 7011 | 3.16 | 379.76 |

- Operations should be O(1)
  - Writing of the results on a file
- Different number of iterations

# Conclusions

- Traffic analysis is non trivial when there are constraints
- Probabilistic model: incorporates most attacks
  - Non-compliant clients
- Monte Carlo Markov Chain methods to extract marginal probabilities
- Future work:
  - SDA based on Bayesian Inference
  - Added value?

# Thanks for your attention

Carmela.Troncoso@esat.kuleuven .be

Microsoft technical report coming soon…

# Bayes theorem

$$\Pr(O, HS \mid C) = \Pr(HS \mid O, C) \cdot \Pr(O \mid C)$$

$$\Pr(O, HS \mid C) = \Pr(O \mid HS, C) \cdot \Pr(HS \mid C)$$

$$\Pr(HS \mid O, C) = \frac{\Pr(O \mid HS, C) \cdot \Pr(HS \mid C)}{\Pr(O \mid C)} = \frac{\Pr(O \mid HS, C) \cdot \Pr(HS \mid C)}{\sum_{HS} \Pr(HS, O \mid C)}$$

Joint probability:

$$\Pr(X, Y) = \Pr(X \mid Y) \cdot \Pr(Y) = \Pr(Y \mid X) \cdot \Pr(X)$$