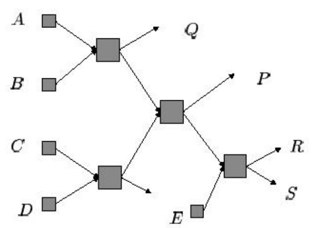
Modeling Entropy in Onion Routing Networks

Danish Lakhani
Anthony Giardullo

Overview

- Global Passive Attacker
- With Some Compromised Nodes
- Want a measure of how much anonymity the network provides

Measuring Anonymity



Anonymous Communication Model

Towards an Information Theoretic Metric for Anonymity [Serjantov, Danezis '02]

A set of all users Ψ in the system

r $\in$ R {sender, recipient} is a role for the user w.r.t. a message *M*

U : attacker's a-priori probability distribution of the users u $\in$ Ψ having the role r w.r.t. message *M*

$$U : \Psi \times R \to [0,1] \quad \text{s.t.} \quad \sum_{u \in \Psi} U(u,r) = 1$$

Entropy (as a measure of anonymity)

An effective (anonymous) set size S of an r anonymity probability distribution U is equal to the entropy of the distribution:

$$S = -\sum_{u \in \Psi} p_u \log_2(p_u) \qquad 0 \le S \le \log_2 |\Psi|$$

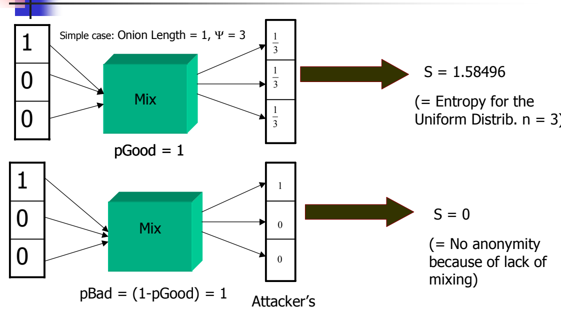
where $p_u = U(u,r)$

-S could be thought of as the number of *additional* bits of information needed by the attacker to completely identify the user *u* with role *r* for a message *M*

- if S = 0, the communication channel is completely compromised

- if S = $\log_2|\Psi|$, the communication channel provides perfect R anonymity

Entropy of Mix Systems



PRISM

- Condition → Action
- Condition →
  prob : Action
  prob : Action
  …

Problems with PRISM

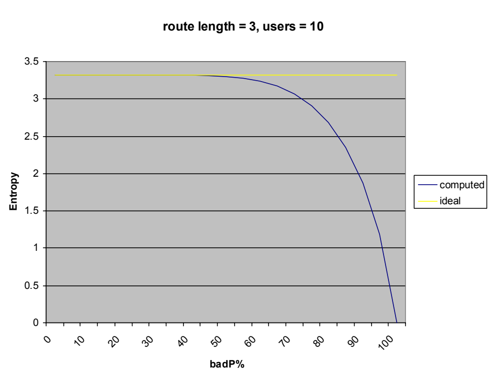
- No Arrays/Data Structures
- Each rule can only have a constant number of transitions
- Sometimes difficult to parameterize

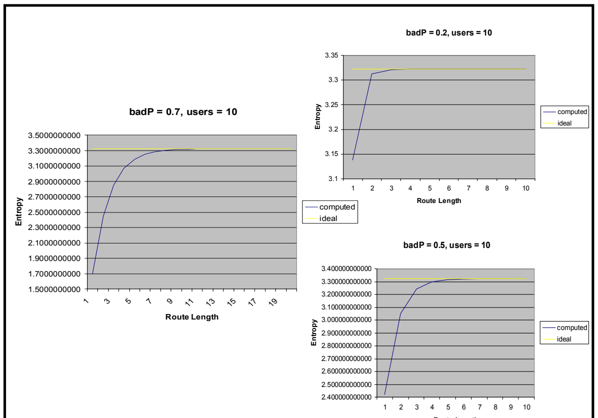
Extend PRISM language

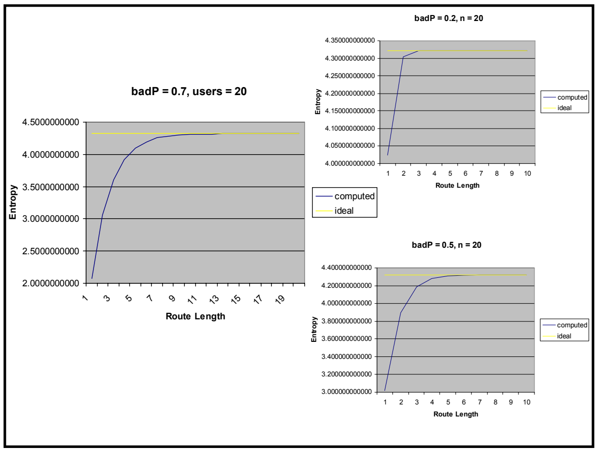
- Added array indexing
- Added For Loops to create many rules
- Created PRISM files with tens of thousands of lines of code

Our First Model

- Fully connected network
- Messages entering good nodes could be sent to every other node with equal probability
- Messages entering bad nodes are sent to a single next node





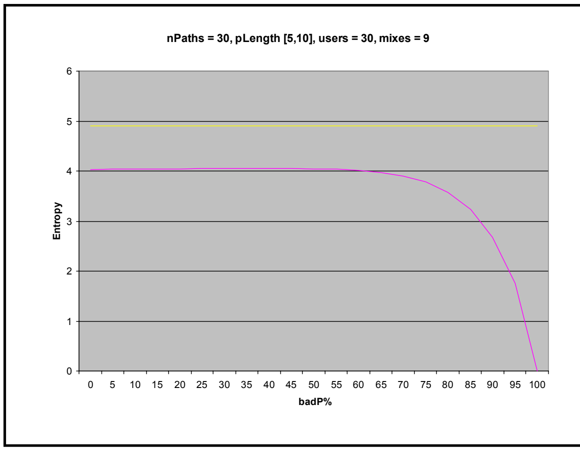


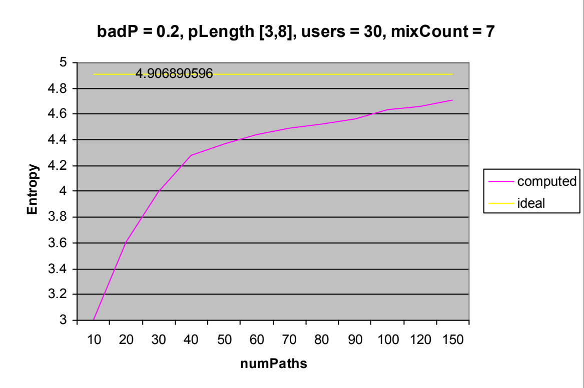
Better Model

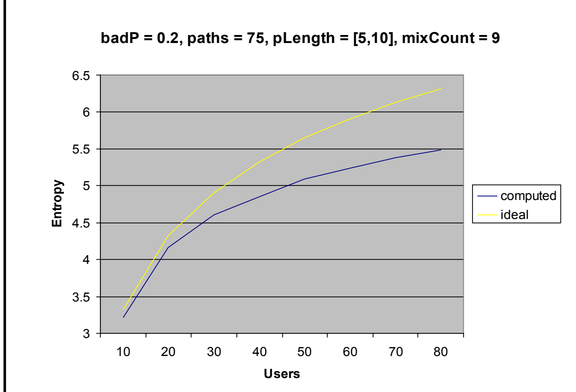
- Model random network traffic
- Assume nodes “mix” traffic
- Generate random multi-graph model

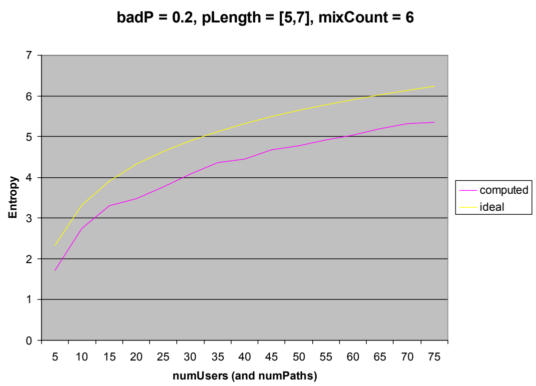
Parameters

- Probability a node is compromised
- Total # messages (paths) in network
- Minimum length of a path
- Maximum length of a path
- Total # users
- Total # mix-nodes
- Random seed









Limitations

- Tried to minimize the number of reachable states in PRISM for our model
- PRISM could only handle up to around 100 nodes with 100 messages

Extending the Model

- Calculate entropy of the system given a maximum and minimum length for all message paths.
- Improved our modeled attacker's knowledge
- Could not improve as much as we wanted to using PRISM

Example