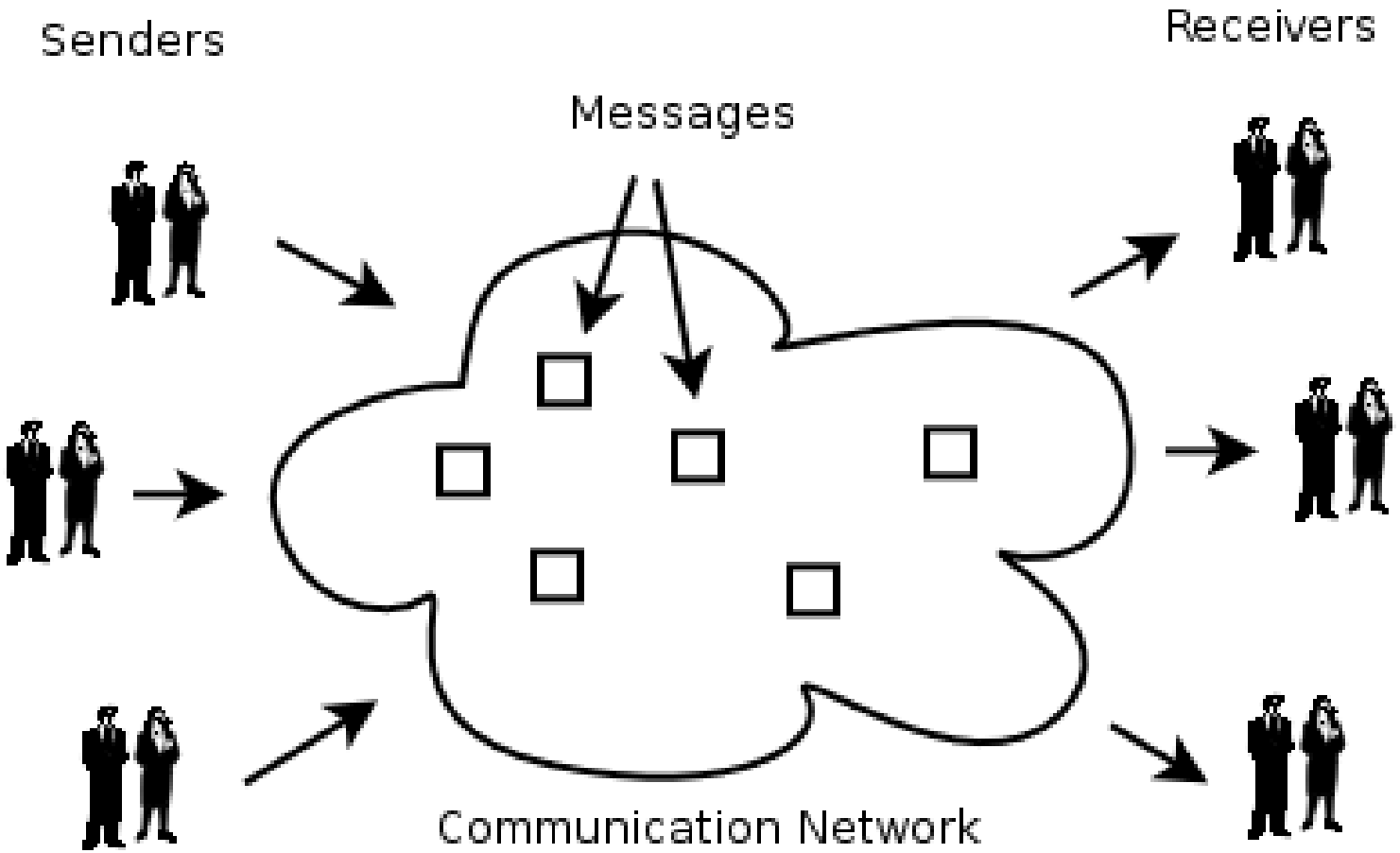
Large Scale Simulation of Tor: Stream Correlation Attacks

Gavin O' Gorman

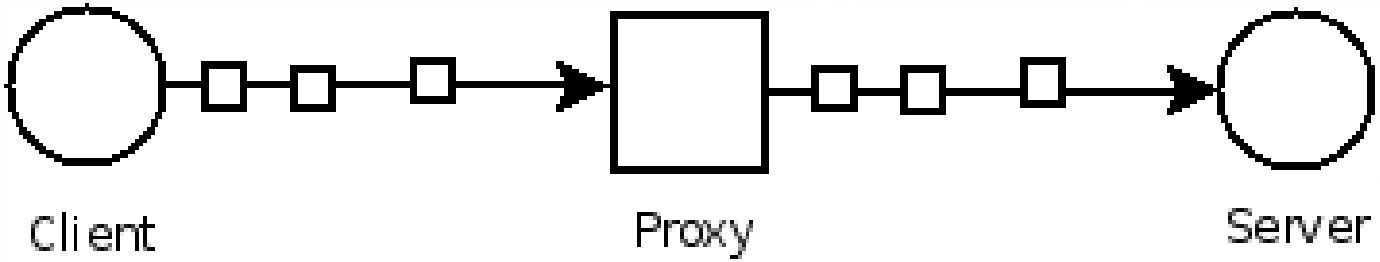
Dublin City University

December 8, 2007

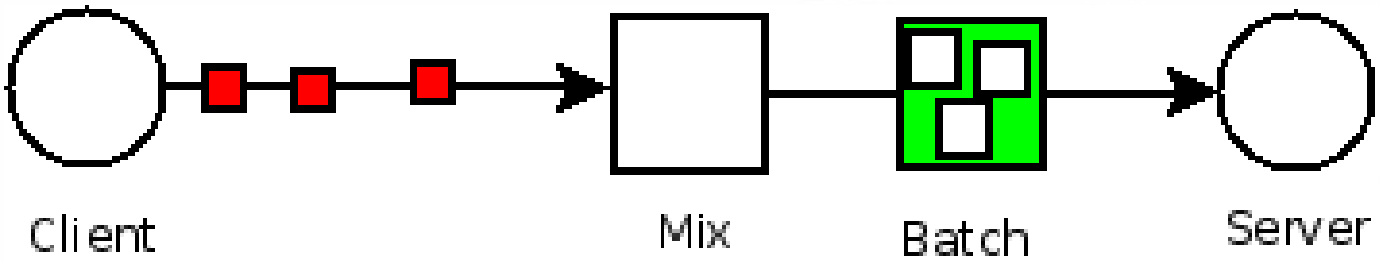
Anonymous networks



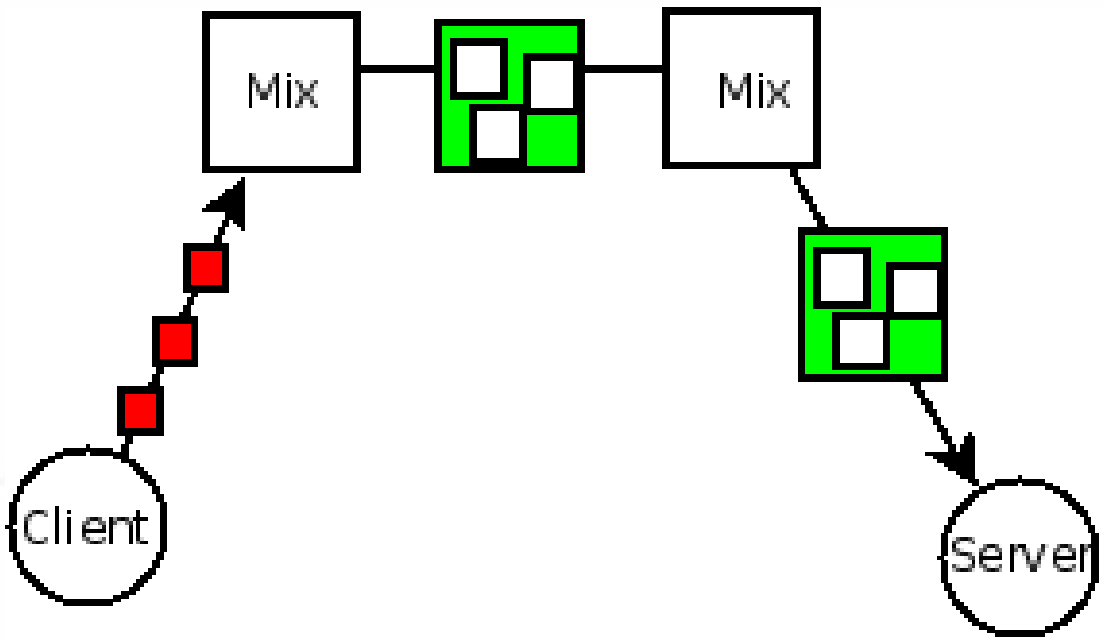
Proxy



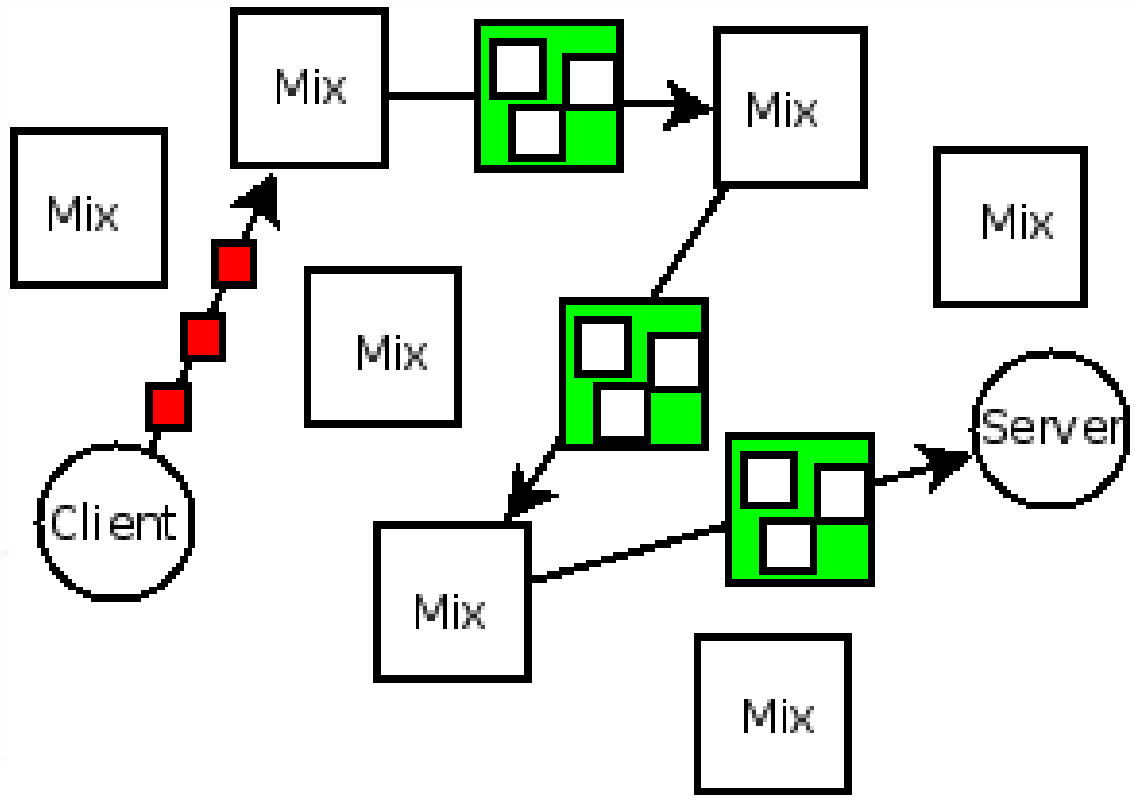
Simple Mix



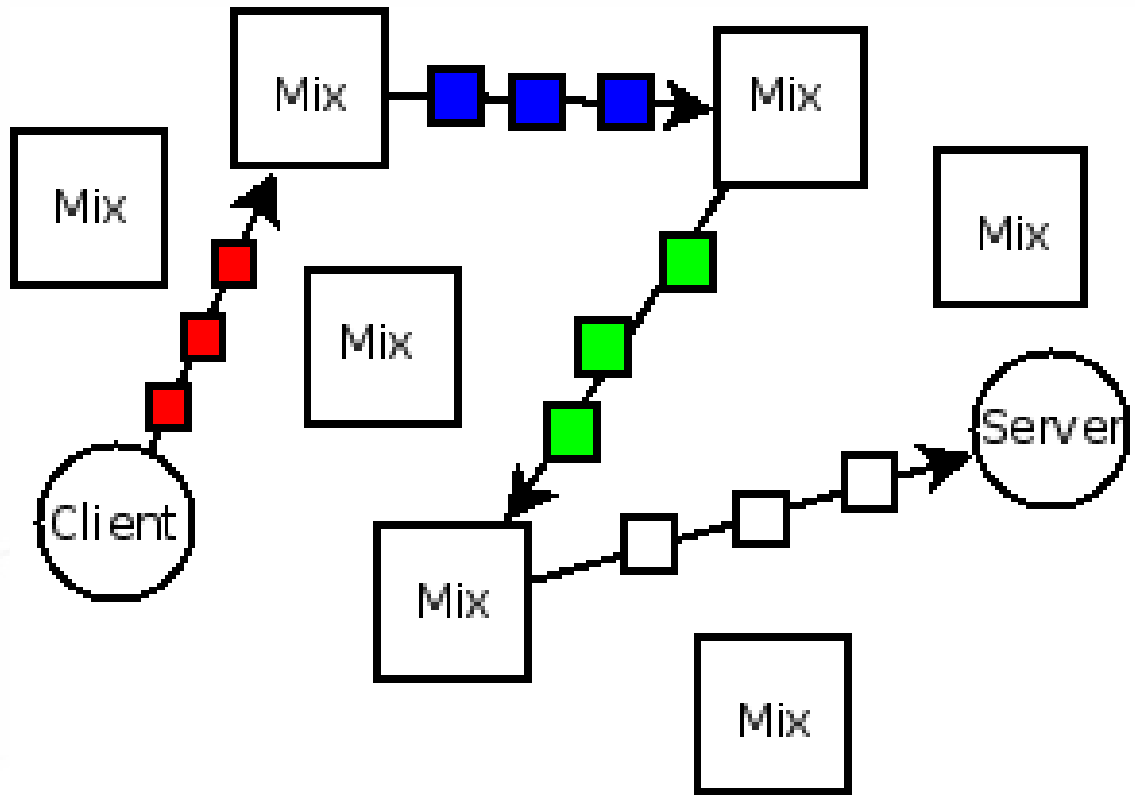
Cascade Mix



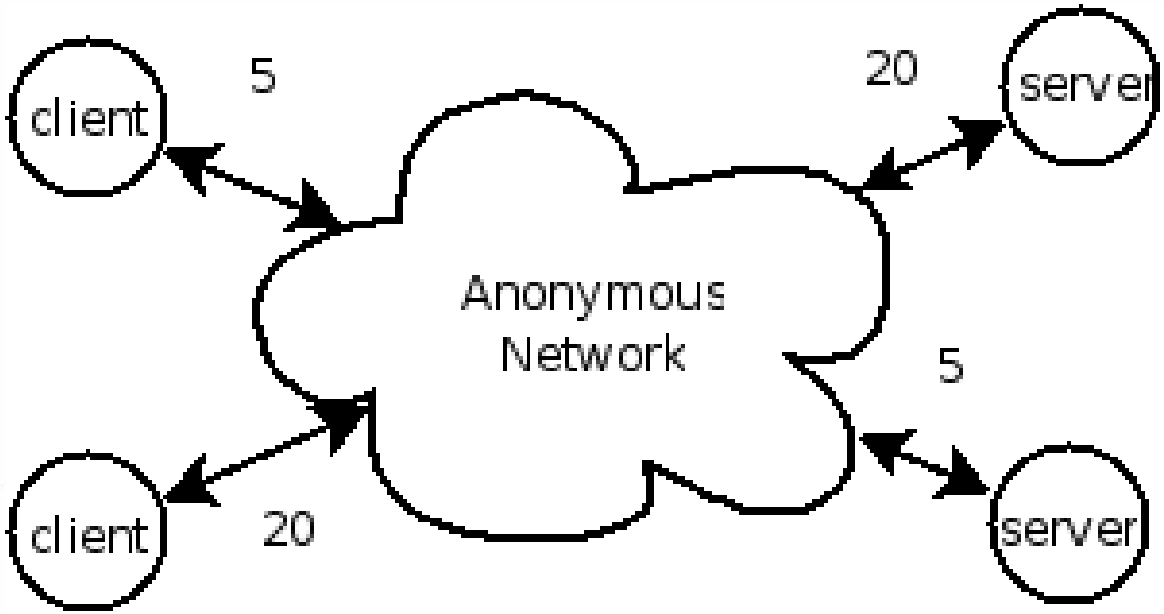
Free Cascade Mix



Low latency network



Traffic Analysis



Currently deployed anonymous networks

- Over 1500 nodes
- Over 100 countries
- Hundreds of thousands on connections through the network
- Theorized traffic analysis attacks

Currently deployed anonymous networks

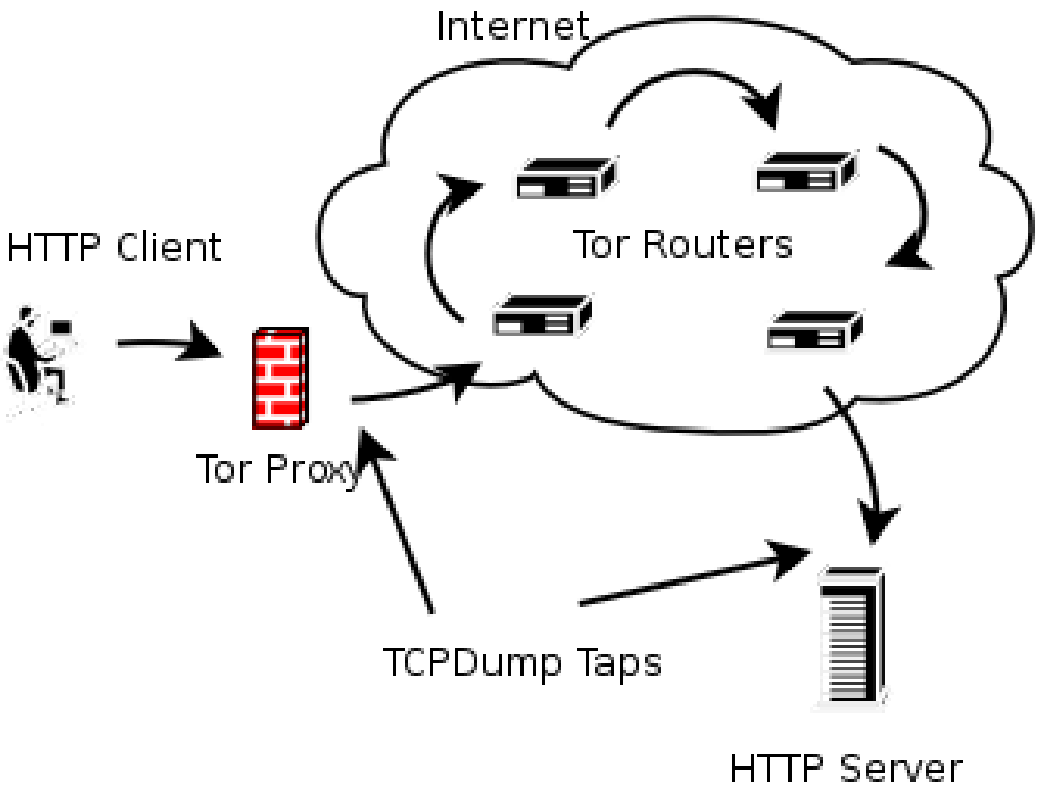
- Over 1500 nodes
- Over 100 countries
- Hundreds of thousands on connections through the network
- Theorized traffic analysis attacks
- How anonymous is a user ?

SSFNet

- Scalable Simulation Framework Network (SSFNet)
- Simulate TCP/IP, Ethernet, Socket interfaces
- Has HTTP/TCP generators.
- TCPDump compatible output

- Simulated Tor circuits, routing, traffic fragmentation
- US ISP Topology
- 6,000 nodes
- Run the simulation for 1060 seconds to settle and then 60 for data

Tor Simulation Process



Results

- Probability of correctly identifying streams entering the network with streams exiting the network
- Several attacks used
  - Start and End timing
  - Packet counting
  - Cross-Correlation - Pearson Function
- Run the attacks with increasing numbers of streams
- Don't know the transit time, so have to test

Start & End stream timing

- Compare the start and end times of streams
- 98% to 94% of streams filtered

Packet counting

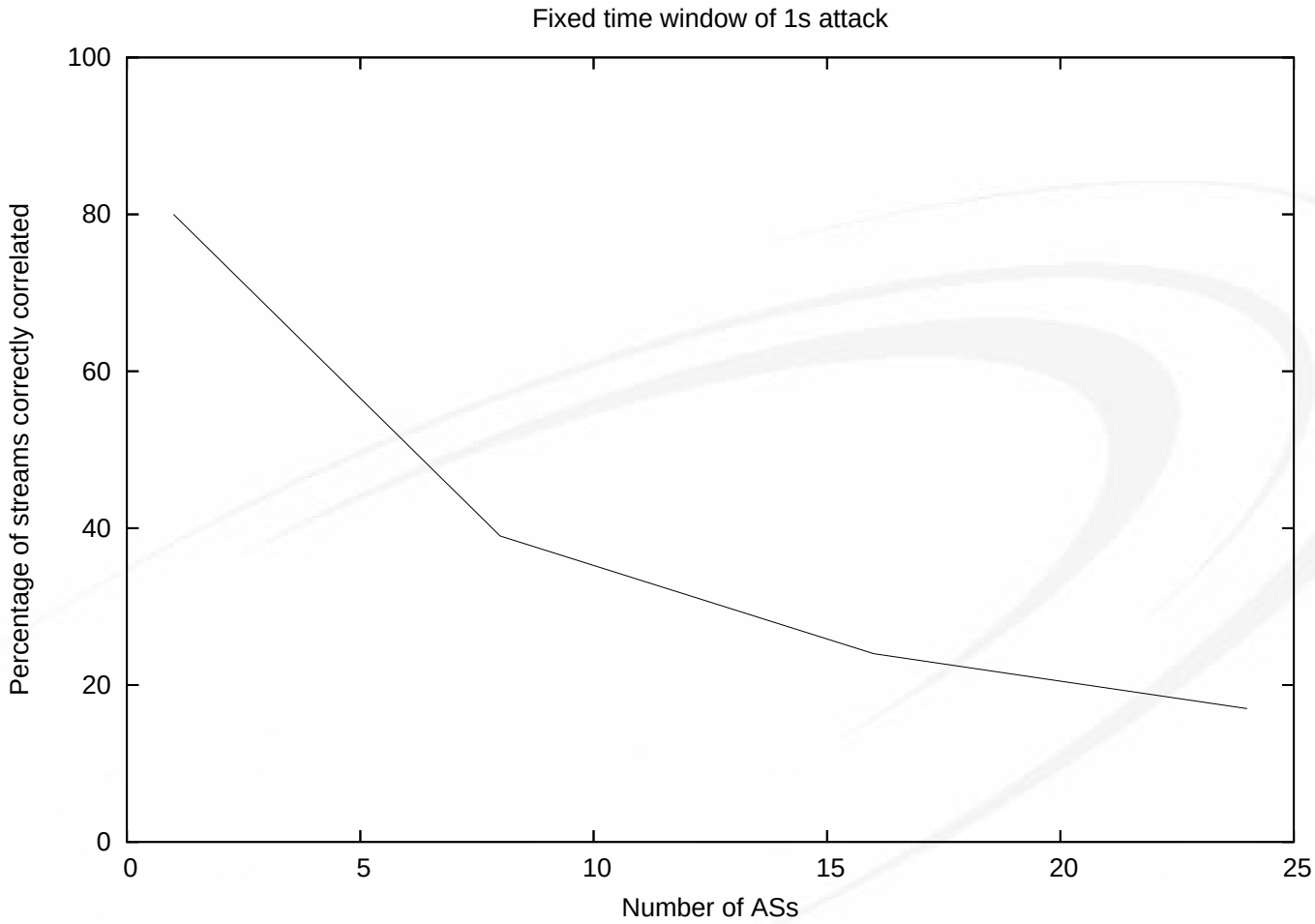
- Count the number of cells in a stream
- 5% to 15% of streams are removed.

Cross-Correlation

$$r(d) = \frac{\sum_i ((x_i - \mu)(x'_{i+d} - \mu'))}{\sqrt{\sum_i (x_i - \mu)^2} \sqrt{\sum_i (x'_{i+d} - \mu')^2}}$$

- Set a windows size W and count the number of packets received
- x_i is the ith packet count of stream x
- x'_i is the ith packet count of stream x'
- μ is the average of packet counts in stream x
- d is the variable delay value

Cross-Correlation



Conclusion

- Initial results show promise
- Future work the simulation will allow us to:
  - Introduce delay and measure QoS & Anonymity
  - Test active attacks
  - Modify Tor protocol to account for specific attacks scenarios

Thank you!

- Thanks for listening and thanks to Science Foundation Ireland

Any questions ?