Exploiting P2P Systems for DDoS Attacks

Keith W. Ross
Polytechnic University

Eric Rescorla's Talk

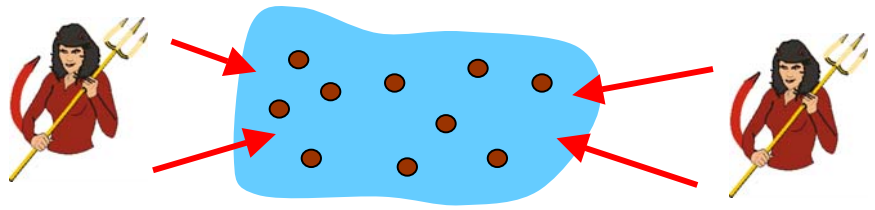
- Data correctness
- Correctness of routing
- Fairness and detecting defection
- DoS

Going to talk about a different attack:

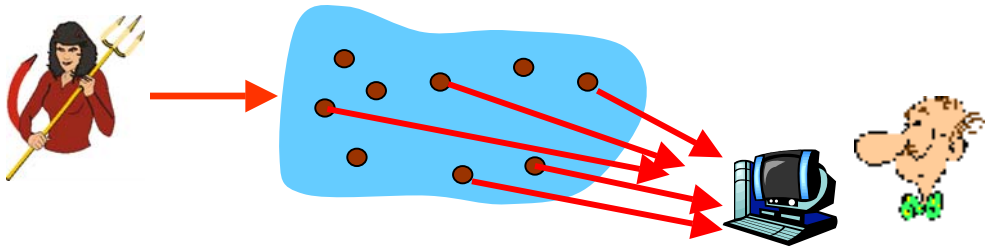
DDoS against arbitrary target

Attacks On & From

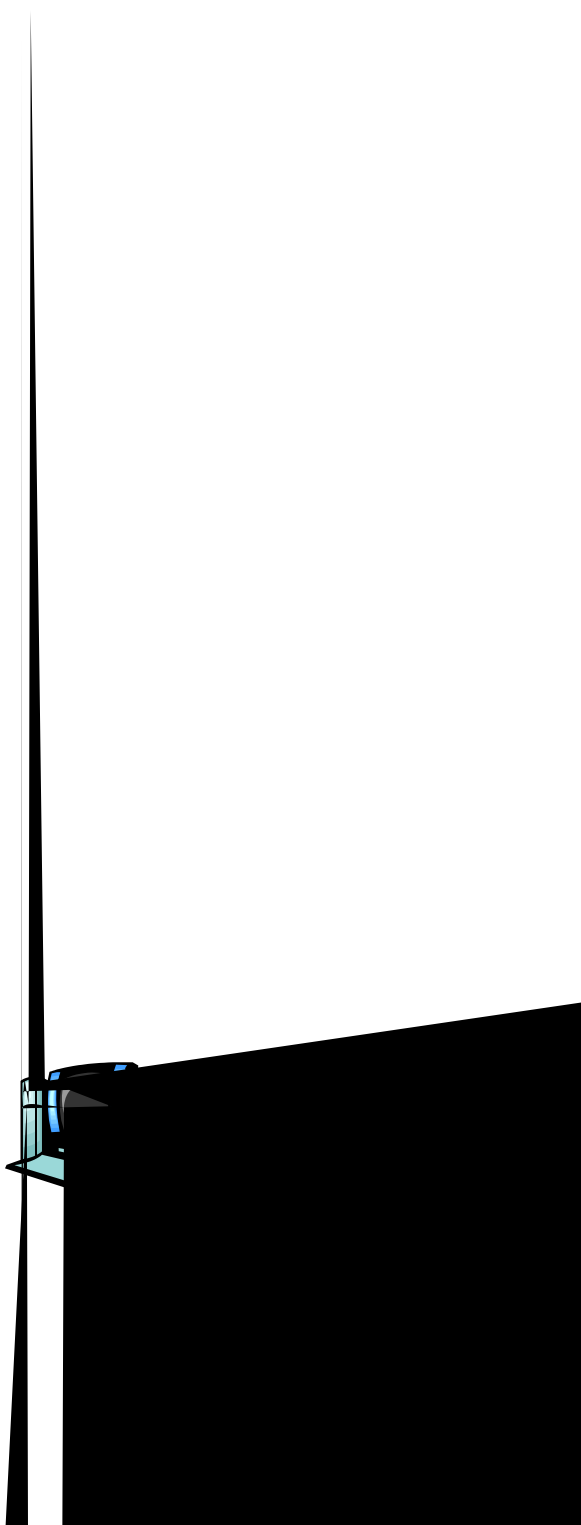
- Attacks <u>on</u> P2P systems:



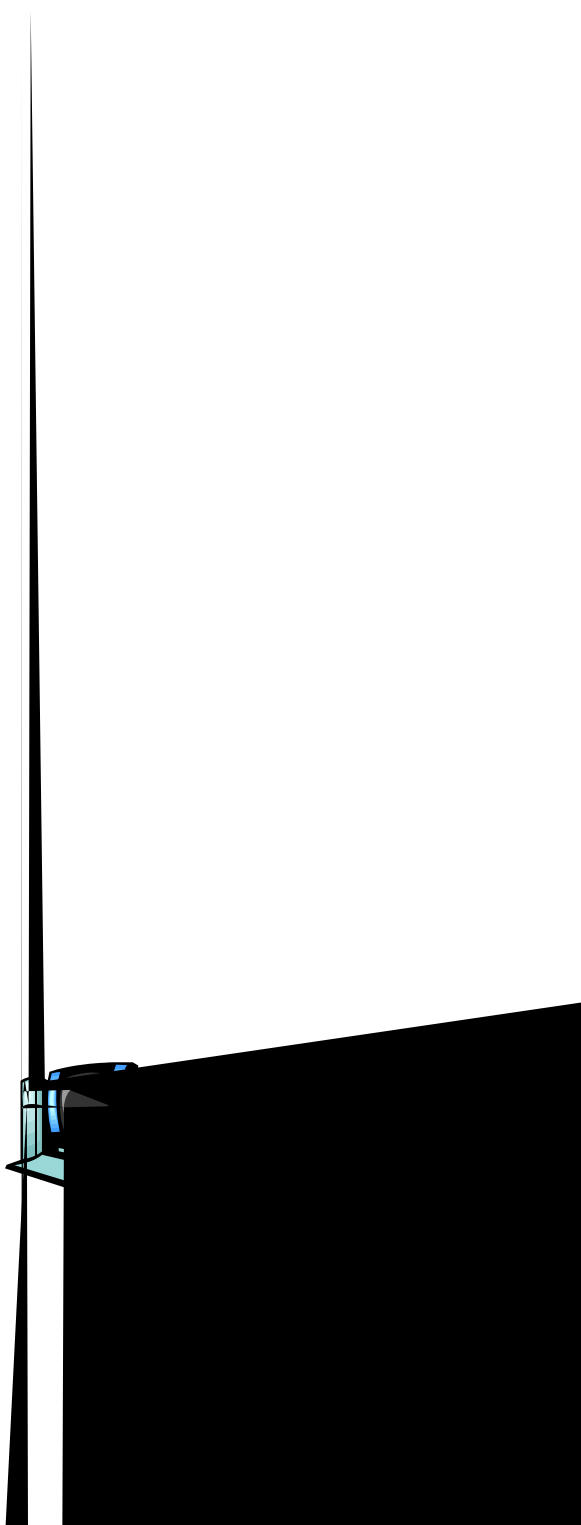
- Attacks <u>from</u> P2P Systems:



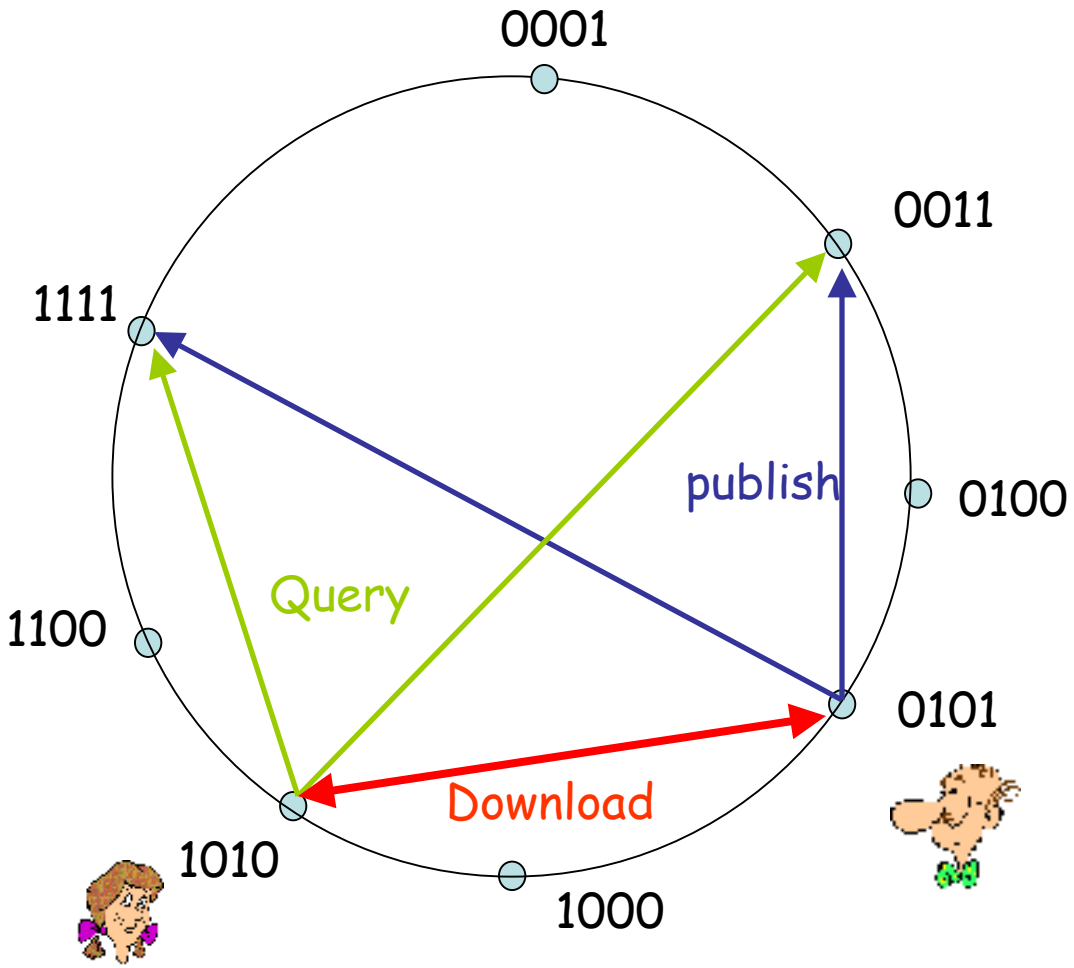
Index Poisoning



Index Poisoning



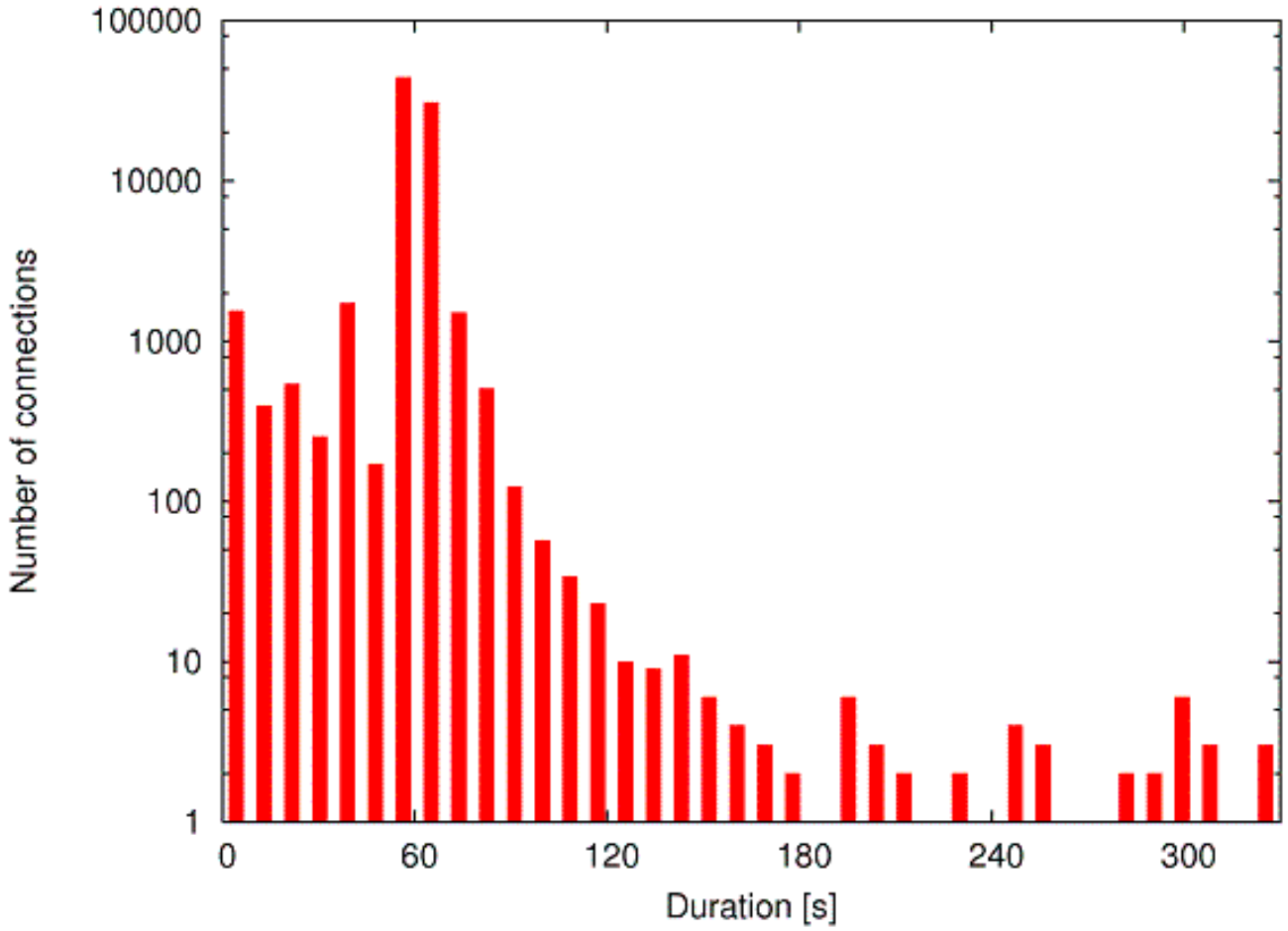
Overnet: DHT


0001
0011
1111
0100
publish
Query
1100
0101
Download
1010
1000

DDoS Attacks From

- Poison distributed index
  - target_IP = www.poly.edu
  - Popular_title = Madonna hit
  - Advertise records: (popular_title, target_IP)
- Users attempt to download popular title
  - Generates fully-open TCP conx's from user peers to target
  - Nastier than syn-flood DDoS attack

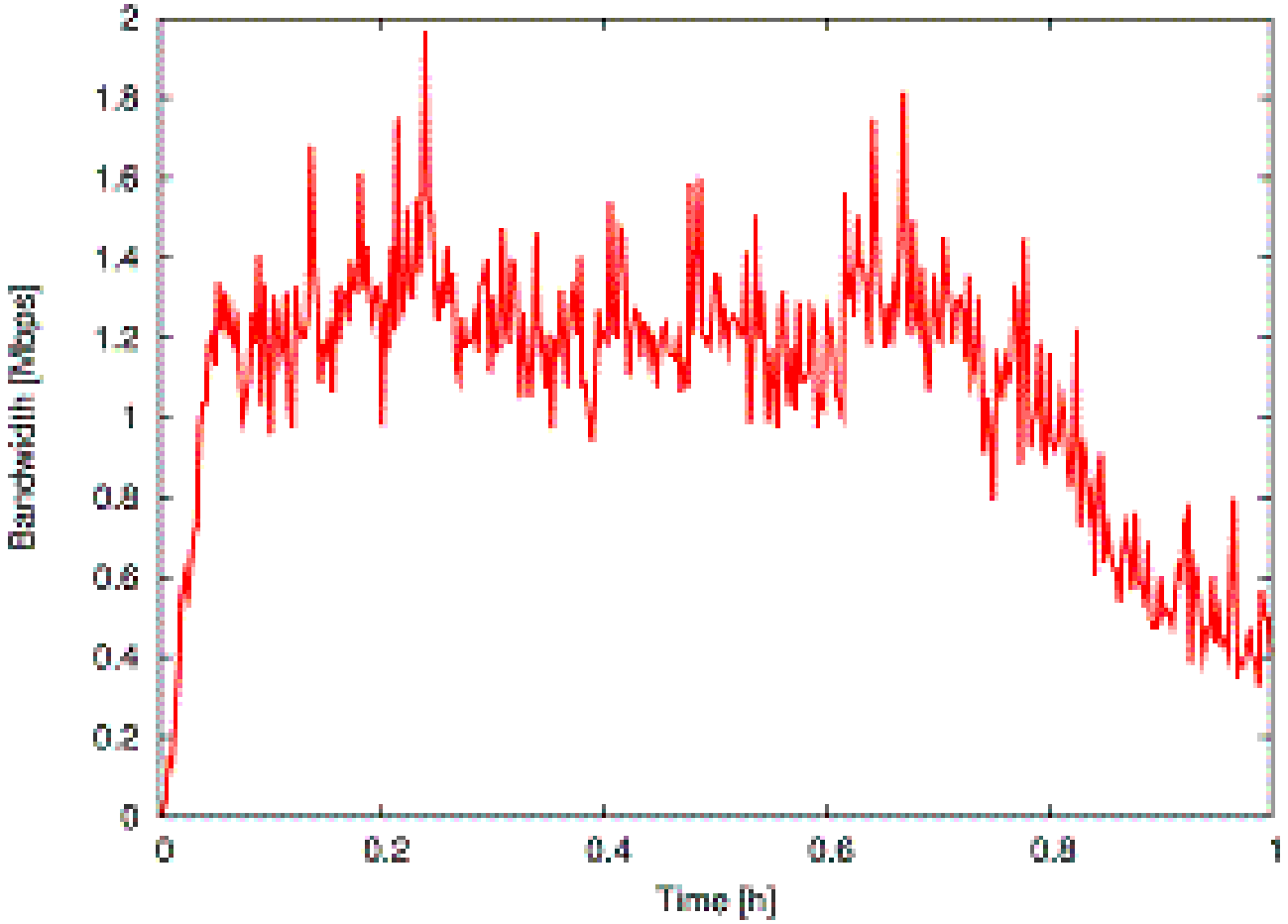
Poison Index: Conx Durations



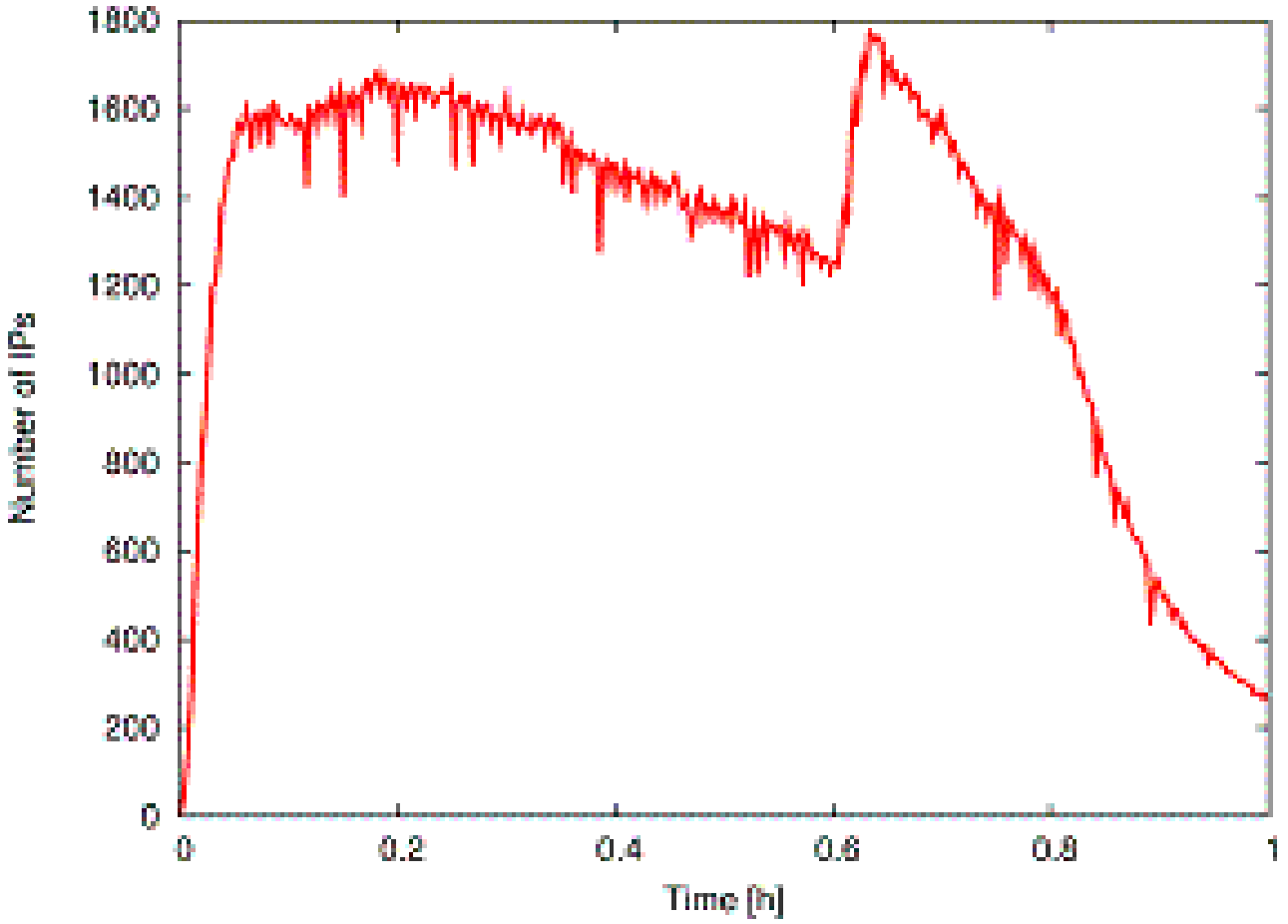
DDoS Attacks From

- Poison overlay routing tables
  - Target = www.ait.edu.th
  - Advertise existence to many nodes: (node_ID, target_IP)
  - Many nodes will absorb advertisement
- Query, publish, overlay messages arrive at poisoned node
  - Some are directed at target

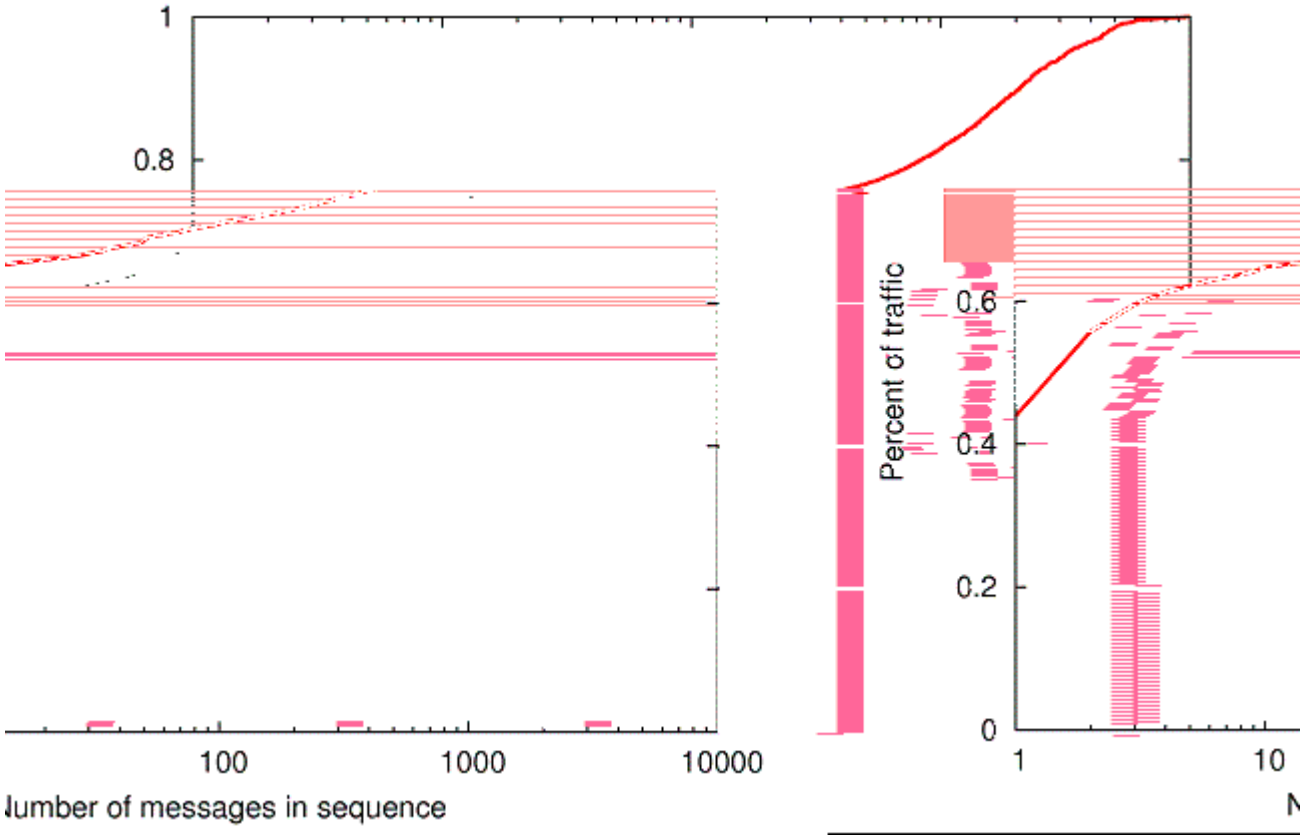
Poison Routing: Bandwidth



Poison Routing: IP sources



Poison Routing Table



Conclusion: DDoS

- Need to be careful!
- Partial solution: verify that advertising node is a node in P2P system