Privacy at the communication layer

Salsa: A Structured Approach to Large-Scale Anonymity. Arjun Nambiar and Matthew Wright 2006

CS-721

Carmela Troncoso
http://carmelatroncoso.com/

Finding nodes is a hard task...

Most of the papers in the previous classes concentrated in how to send messages, and what happened once routes are chosen.

Yet in Tor / Crowds plenty of our discussion went into node lookup!

Also we talked about

"Bridging and Fingerprinting: Epistemic Attacks on Route Selection"
Danezis & Syverson

That showed how important node knowledge is.

Salsa is more about how to find nodes than about how to use them for anonymity.

What we have seen so far

Tor: the directory authority makes available the list of all nodes in the system

Crowds: the directory authority makes available the list of all nodes in the system

DC networks: not even mentioned... everybody knows everybody

Others

Tarzan:

Tarzan: A Peer-to-Peer Anonymizing Network Layer

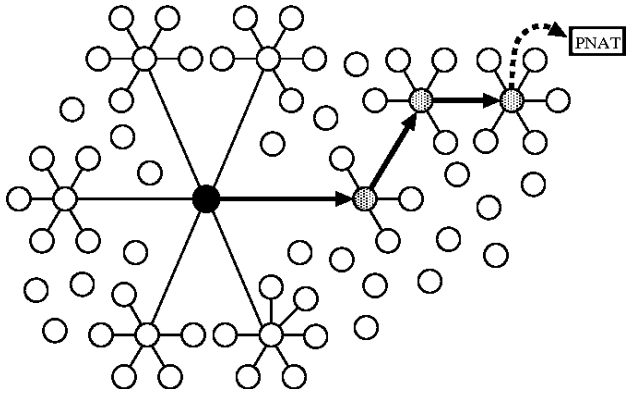
Michael Freedman and Robert Morris, 2002

Core principle: **Me relay, you relay** (by M. Freedman)

- difficult to block everyone (censorship resistance)
- cover traffic for all
- no edges of the network, no first node

CROWDS

Layered encryption (not exactly onion routing)
Final NAT ("Pseudonymous NAT") to connect to exterior
Cover traffic – "mimic" nodes exchange traffic
Source-based routing through mimics



Node discovery

– "Gossiping": nodes ask neighbours for nodes
from weakly connected to fully connected

Need full connection to
Avoid biases and leaks

Node selection

– limited to domains: avoid easy control of paths

What we have seen so far

Tor: the directory authority makes available the list of all nodes in the system

Crowds: the directory authority makes available the list of all nodes in the system

DC networks: not even mentioned... everybody knows everybody

Others

Tarzan: peers discover all peers via gossiping

MorphMix

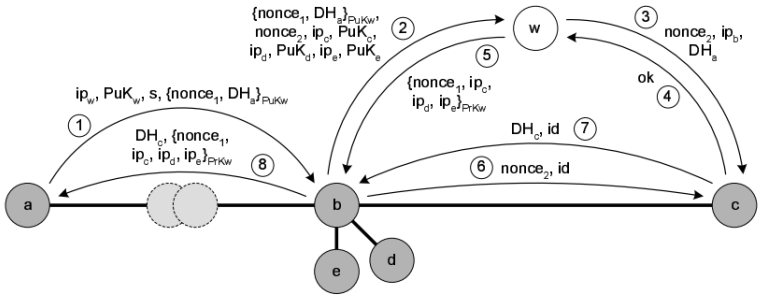
Introducing MorphMix: Peer-to-Peer based Anonymous Internet Usage with Collusion Detection

Marc Rennhard and Bernhard Plattner, 2002

Non-source routed (Crowds-like)

- No lookup needed (only neighbours) -> scalable
- What if first is an adversary?
  - Attacker nodes appear more often: Witness to collect offered nodes

Layered encryption (not exactly onion routing)



Node discovery

- Memory: try nodes you knew last time
- Server nodes
  - distribute "some" nodes (always random)
  - use several servers to avoid attacks
- Also from offered extensions

What we have seen so far

Tor: the directory authority makes available the list of all nodes in the system

Crowds: the directory authority makes available the list of all nodes in the system

DC networks: not even mentioned... everybody knows everybody

Others

Tarzan: peers discover all peers via gossiping

MorphMix: peer needs to know few nodes

What we have seen so far

Tor: the directory authority makes available the list of all nodes in the system

Crowds: the directory authority makes available the list of all nodes in the system

SCALABILITY

DC networks: not even mentioned... everybody knows everybody

Others

Tarzan: peers discover all peers via gossiping — Scalability, Intersection attacks

MorphMix: peer needs to know few nodes — Sybil attacks

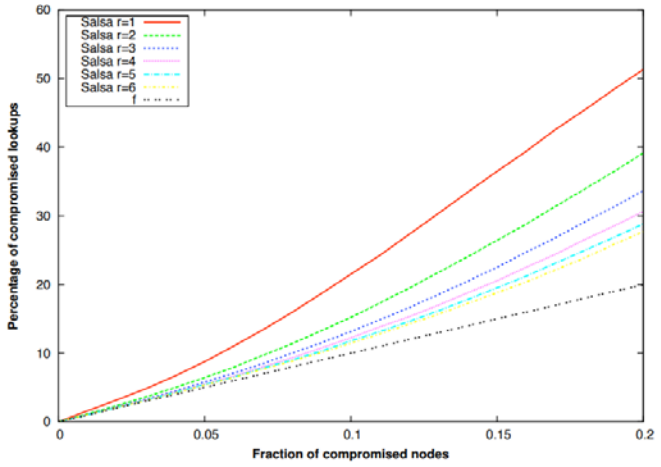
Salsa: know few nodes and redundancy anti-sybil

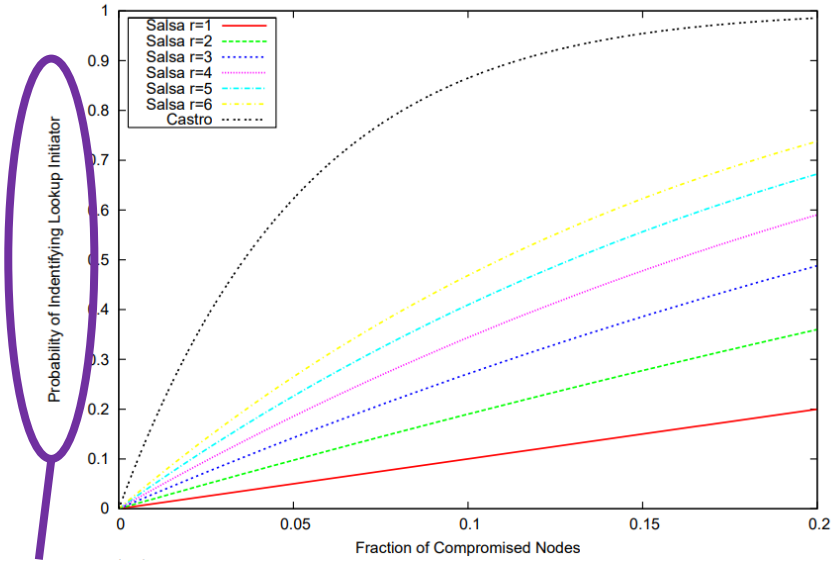
Redundancy → more information

Redundant lookups: protect against active adversaries

↓

But leave more information to passive adversaries





The more redundancy, more likely one of searches is run by a malicious node

NO ANONYMITY FOR THE LOOKUP!

Prateek Mittal and Nikita Borisov. Information Leaks in Structured Peer-to-peer Anonymous Communication Systems. ACM Conference on Computer and Communications Security (CCS 2008).

Redundancy → more information

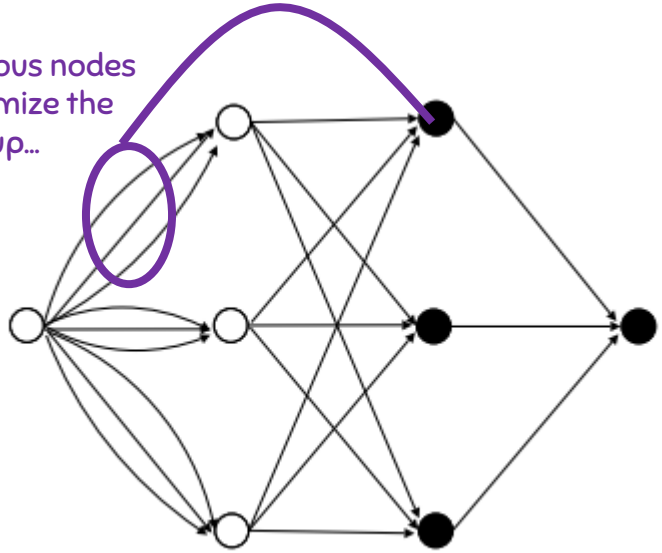
Anonymity of communication

↓

Nodes in the second level do not know initiator

One node per level compromised (redundancy ↑ probability)

If the malicious nodes de-anonymize the lookup...



(a) Bridging an honest first stage

Prateek Mittal and Nikita Borisov. Information Leaks in Structured Peer-to-peer Anonymous Communication Systems. ACM Conference on Computer and Communications Security (CCS 2008).

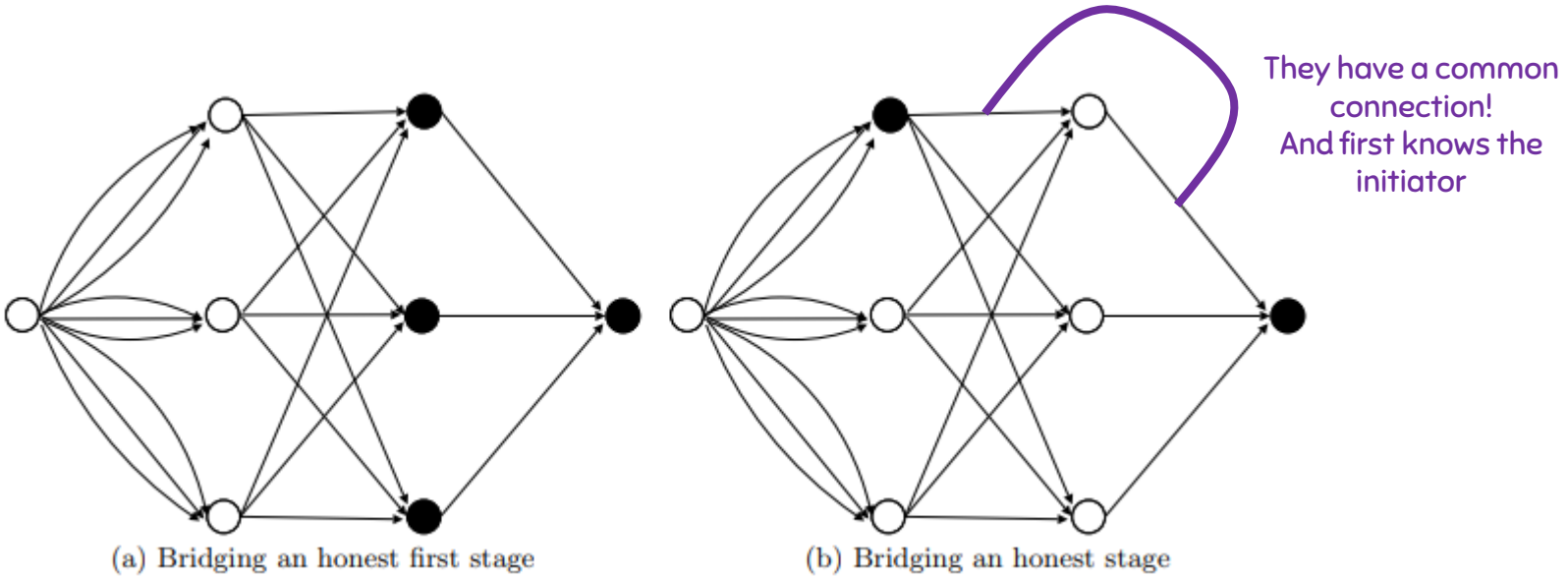
Redundancy → more information

Anonymity of communication

↓

Nodes in the second level do not know initiator

One node per level compromised (redundancy ↑ probability)



(a) Bridging an honest first stage

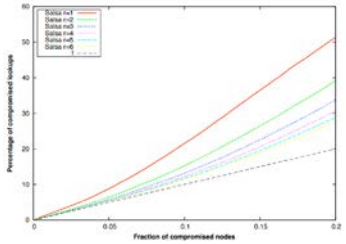
(b) Bridging an honest stage

Prateek Mittal and Nikita Borisov. Information Leaks in Structured Peer-to-peer Anonymous Communication Systems. ACM Conference on Computer and Communications Security (CCS 2008).

AP3 = Crowds + secure lookup

A. Mislove, G. Oberoi, A. Post, C. Reis, P. Druschel, and D. S. Wallach, 2004

Crowds analysis = Pr[next to initiator]



Non-anonymous Lookups

Information about lookups help identifying the predecessor!

Prateek Mittal and Nikita Borisov. Information Leaks in Structured Peer-to-peer Anonymous Communication Systems. ACM Conference on Computer and Communications Security (CCS 2008).

NISAN: NETWORK INFORMATION SERVICE FOR ANONYMIZATION NETWORKS

ANDRIY PANCHENKO, ARNE RACHE, AND STEFAN RICHTER, 2009

🤔 THE PROBLEM WITH NON ANONYMOUS LOOKUPS IS THAT THE ADVERSARY LINKS

SENDER – NODE SOUGHT

LET'S HIDE THE NODE SOUGHT!!

ASK NODES FOR THEIR FINGER LIST INSTEAD OF THE TARGET

1. ASK FINGERS FROM TOP LIST OF CANDIDATES
2. IF A FINGER IS NEARER, PUT IN TOP LIST
3. REPEAT UNTIL LIST DOES NOT CHANGE

NISAN: NETWORK INFORMATION SERVICE FOR ANONYMIZATION NETWORKS
ANDRIY PANCHENKO, ARNE RACHE, AND STEFAN RICHTER, 2009

LET'S HIDE THE NODE SOUGHT!!

ASK NODES FOR THEIR FINGER LIST INSTEAD OF THE TARGET

1. ASK FINGERS FROM TOP LIST OF FINGER CANDIDATES
2. IF A FINGER IS NEARER, PUT IN TOP LIST
3. REPEAT UNTIL LIST DOES NOT CHANGE

BUT THE LISTS REVEAL INFORMATION!

IF YOU ARE ASKED: YOU ARE A PREDECESSOR OF TARGET
IF YOUR FINGERS ARE NOT ASKED: THEY ARE SUCCESSORS OF THE TARGET

Qiyan Wang, Prateek Mittal, and Nikita Borisov. In Search of an Anonymous and Secure Lookup: Attacks on Structured Peer-to-peer Anonymous Communication Systems . ACM Conference on Computer and Communications Security (CCS 2010).

Takeaways

- Node discovery is difficult
  - Scalability
  - Sybil prevention
- Fixing problems.... May add more problems
  - More interactions result in more information
- Solutions:
  - Anonymity in lookup (Torsk, take a look)
  - Private information retrieval (Tor-alike)

Anonymous communications to protect anonymity

Can do more: censorship resistance

Next week

Telex: Anticensorship in the Network Infrastructure