TARZAN: A PEER-TO-PEER ANONYMIZING NETWORK LAYER

Presented by;
Shaun Deaton

Tarzan is an anonymization tool providing, under the assumption of an X adversary, the following:

- Sender & recipient anonymity
  - Both give relational anonymity, where only one needs to be running Tarzan
- Distributed trust via unbiased peer selection
  - Actually seemed biased since candidate nodes checked against validated nodes

X = passive group, legal, net back-bone access, local, global…

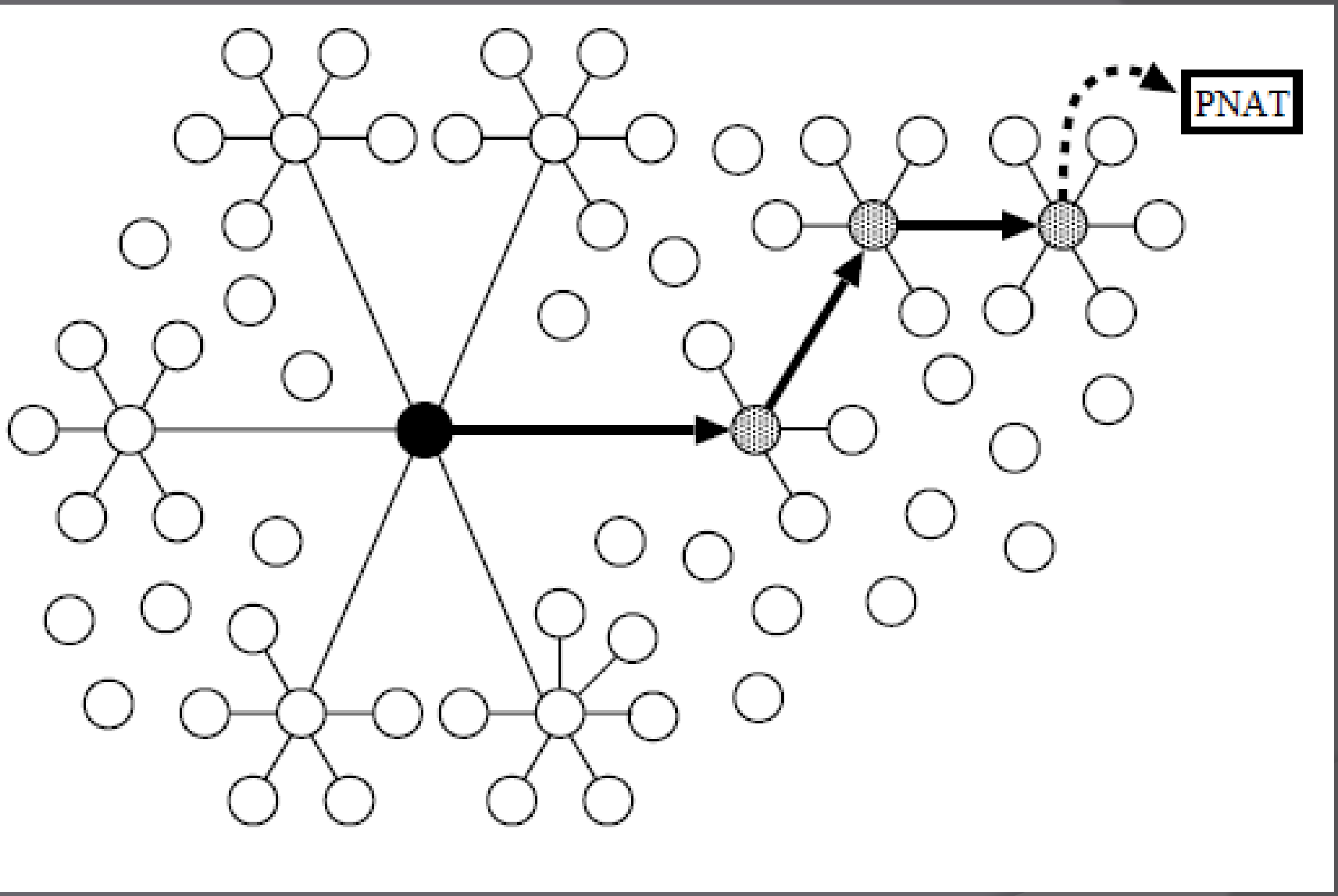
- Server-side pseudo-anonymous network address translator
  - PNATs are the destinations of mimic sequences
- Integrity checking using nested hashes of addresses and time/date
  - Hashes used as neighborhood comparison to improve Name-Dropping scheme

- Absence of a central coordinating entity
  - Connections built dynamically
  - Change overtime
- Built in transport layer
  - Transparent to apps
  - “abstraction of an IP tunnel”

- Domain level view, opposed to node level
  - Assume adversaries can control entire subnets
  - Selects relay nodes across domains
- Mimics
  - Which seems to be another node sharing a special kind of traffic with the other; “mimic traffic”
  - Mimic traffic “indistinguishable from cover traffic”
  - Mimics require cover traffic
  - Not certain what they actually are …

“Tarzan introduces a scalable and practical technique for **cover traffic** that uses a restricted topology for packet routing: Packets can be routed only between **mimics**, *or pairs of nodes assigned* by the system in a secure and universally-verifiable manner”

- Tunnels
  - Choose sequence of nodes & get public keys
  - Generate corresponding symmetric keys to encrypt & distribute
  - Distinguishes between validated & invalidated addresses/keys by the say-so of at least one trusted peer
  - Creates a path of handshaking asymmetric encryptions among mimic relays that each use the symmetric key of the originator in an onion


PNAT

Assumes out-of-band secure communication channel, at least to start the network.

- Needed to provide initial trusted nodes to have a foundation for verifiability
- Cannot start with a random set of starting nodes to form network when joining is anonymous & unrestricted.

Node key validation should be built on more than essentially just the minimum of one other node’s say-so

- Similar reasoning behind using domain level over node level
- Nodes that are PNATs seem to have a special status; so should their public keys have also?

……

END of coverage

Note:

- “All packets along these mimics links are symmetrically encrypted. This encryption—an additional layer on top of the tunnel encoding—makes cover traffic indistinguishable from data flows.”
- “Encrypted packets along these links are padded to be all the same size. A node generates and distributes symmetric keys when it connects with a new mimic.”

“Tarzan should resist an adversary’s attempts to overload the entire system or to block system entry or exit points”

“Tarzan should minimize the damage any one adversary can cause …”