Kaleidoscope: social networks stymie censors

Jinyang Li, http://www.news.cs.nyu.edu/kalei

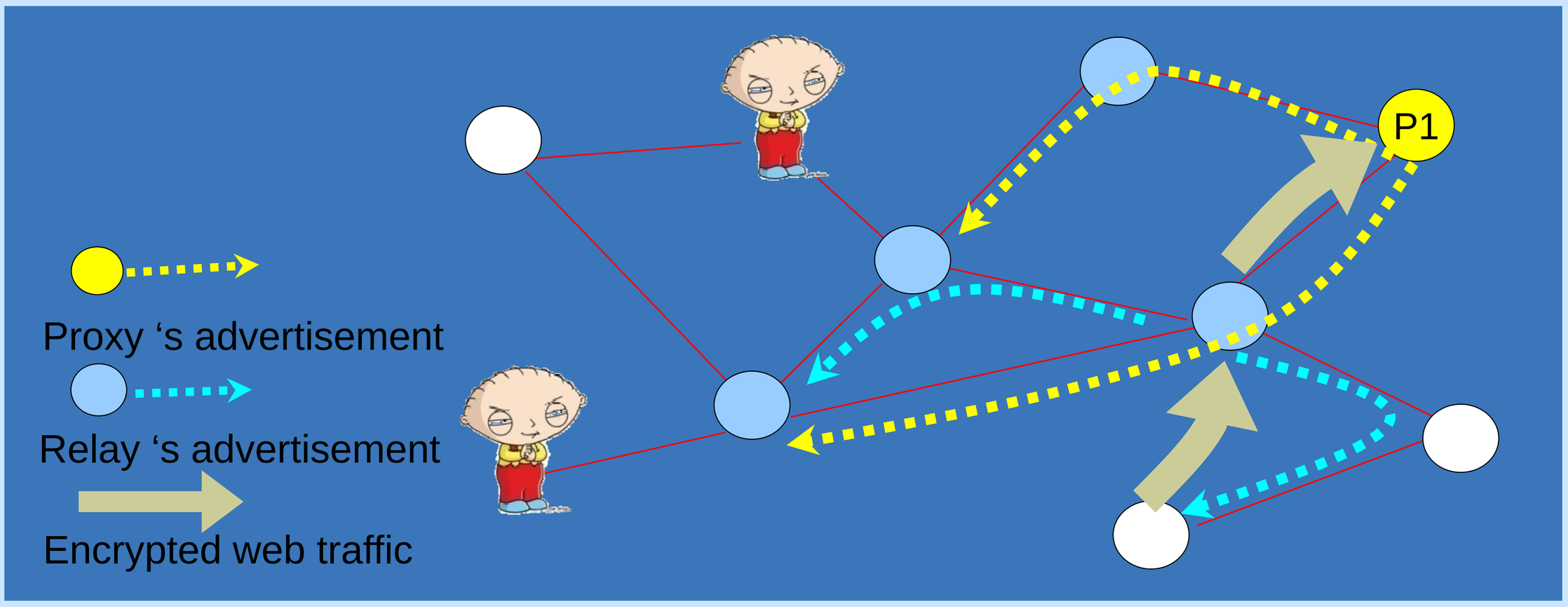
NSF grant CNS-0747052

Problem & Challenges

Many countries block access to *grey* materials. To access blocked contents, users can relay traffic via an unblocked proxy. We address the challenge of helping users discover proxies' addresses while shielding them from the radar of the censor.

Kaleidoscope's approach

- Disseminate proxy addresses over a p2p overlay whose links reflect real world trust relationships between users.
- Ensure each node learns only a small subset of proxies. As the censor is unlikely to infiltrate a large fraction of users, he cannot discover many proxies.



New approach

- Leverages social trust to mitigate the Sybil attack
- Limit how much a user can learn of other nodes

Impact

- Help users in censored domain access blocked material
- Demonstrate new ways to build decentralized systems using trust

Technical Description

- Kaleidoscope forwards proxy advertisements using *short* random routes [Yu et al.]. Each node constructs a routing table mapping each incoming link to a randomly chosen outgoing link and forwards advertisements accordingly. Short random routes guarantee that a proxy is only known to a small number of nodes *and* that no decoy proxy can advertise itself to many nodes.
- Relay nodes forwards traffic to known proxies. Relays advertise their own addresses to help the system serve more users without requiring proxies to advertise to more nodes.

- Simulation results show more than 85% users have unblocked proxy service even when 2% users collude with the censor and act as informants . We used routes of length 10.

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Cyber Trust Principal Investigators Meeting
March 16-18, 2008
New Haven, CT

New York University