A Technical Approach to Net Neutrality

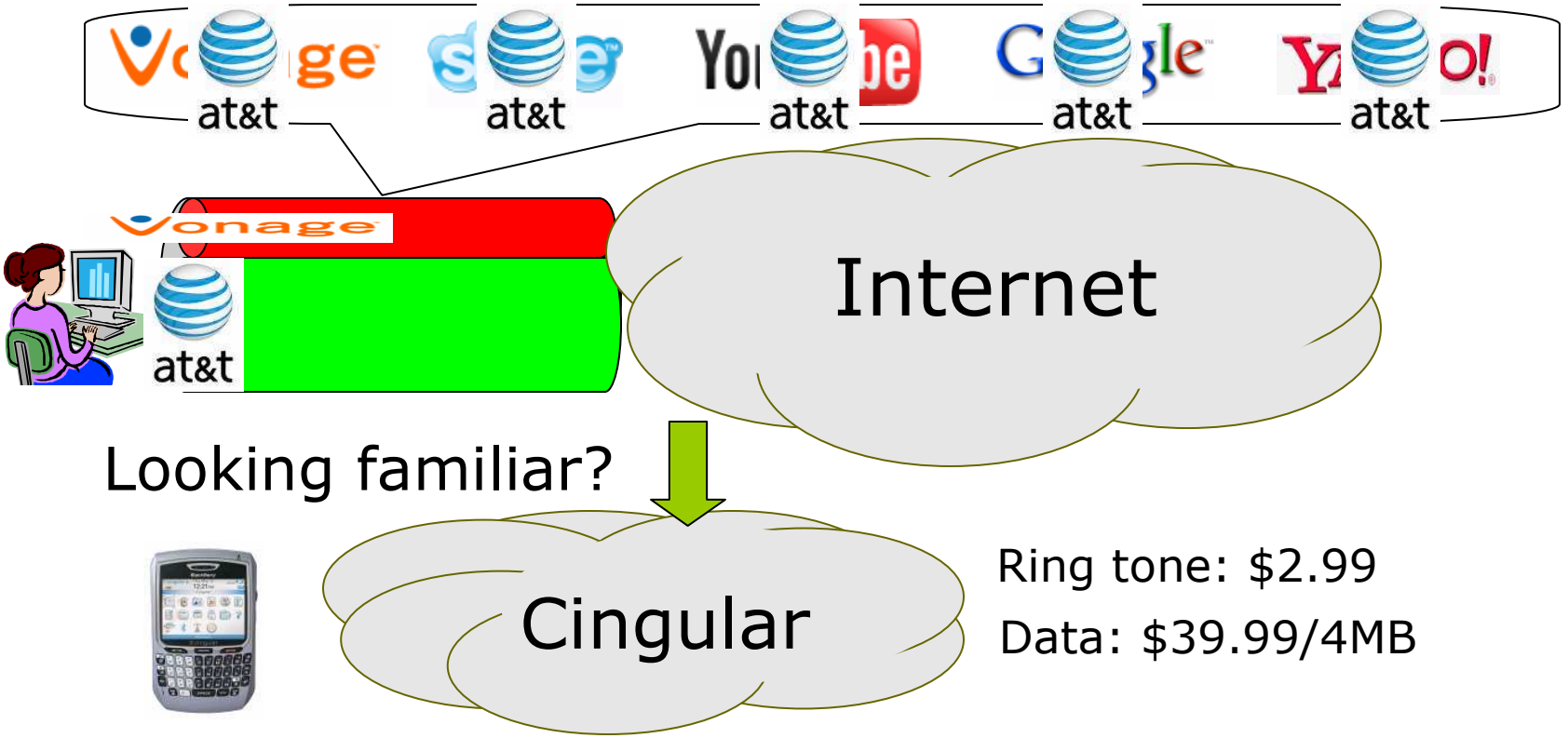
Xiaowei Yang and Gene Tsudik and Xin Liu
Department of Computer Science
UC Irvine
http://www.ics.uci.edu/~xwy/publications/neutralizer.pdf

Their Plan

- In November 2005, AT&T CEO (formerly SBC CEO) Ed Whitacre was quoted in **BusinessWeek** as follows [3]:

  "Now what they [Internet upstarts like Google, MSN, Vonage, and others] would like to do is use my pipes free, but I ain't going to let them do that because we have spent this capital and we have to have a return on it," says Whitacre. "So there's going to have to be some mechanism for these people who use these pipes to pay for the portion they're using. Why should they be allowed to use my pipes?"

Our Fear



- Ex. "Comcast, the largest USA Broadband provider is being accused of VoIP blocking, just days before they release their own VoIP offering." (March, 2006, http://slashdot.org/articles/06/03/02/139241.shtml)
- "Whether acting as a bottleneck, a toll-taker, or a gatekeeper, the broadband carriers propose to transform the Internet into something akin to a closed and proprietary system of centralized control." Vint Cerf, June 14, 2006

Concerns over regulatory steps

- Difficulties to draw the line
  - "If a broadband network provider prioritizes or offers enhanced quality of service to data of a particular type, it must prioritize or offer enhanced quality of service to all data of that type (regardless of the origin or ownership of such data) without imposing a surcharge or other consideration for such prioritization or enhanced quality of service." *from* ***Freedom and Nondiscrimination Act of 2006***
  - **"**only prioritize content, applications, or services accessed by a user that is made available via the Internet within the network of such broadband service provider based on the type of content, applications, or services and the level of service purchased by the user, without charge for such prioritization" *from* ***Internet Freedom Preservation Act of 2006 (Snowe-Dorgan bill)***
- A violation of free-market policy
- No strict net neutrality regulation has established

Our position

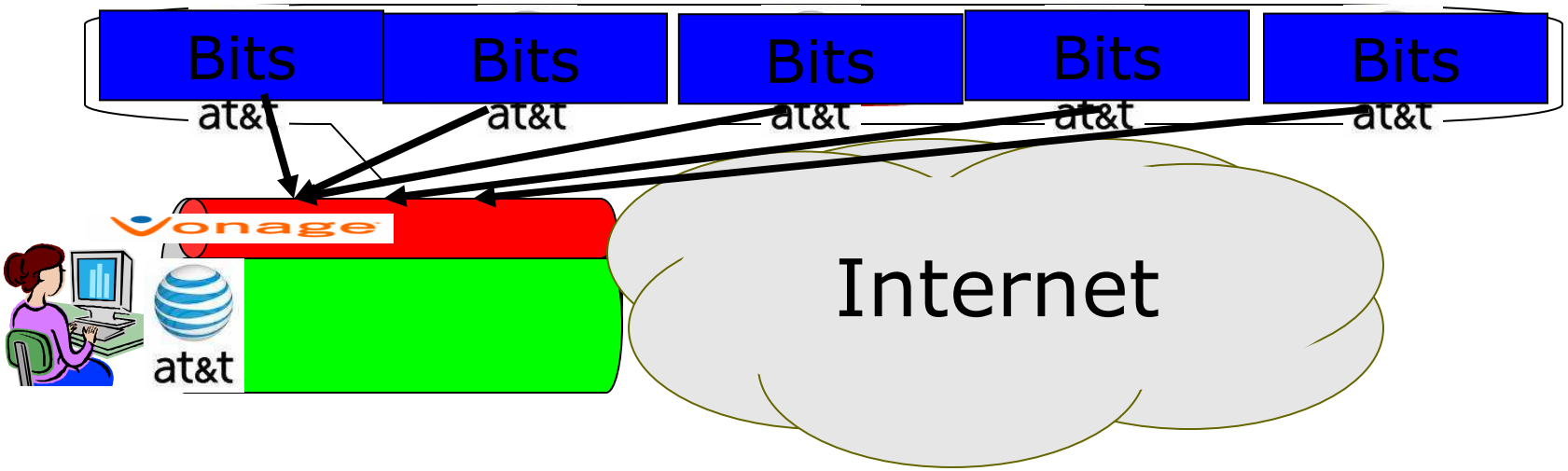
- We cannot afford losing the openness of the Internet, and the pros and cons of regulation are hard to tell.

- An alternative to regulation is to design a clean QoS interface such that data prioritization cannot be based on contents, application types, or non-customer ends of data.

Design goal

- Allow differentiated services at network layer
  - Customers may purchase capacity (or traffic profile) at different prices
  - Customers decide how to use the services
- Prevent network-enforced data prioritization based on
  - Contents
  - Application types
  - The non-customer ends of data
    - Always face a monopoly

Key idea: blur all packets



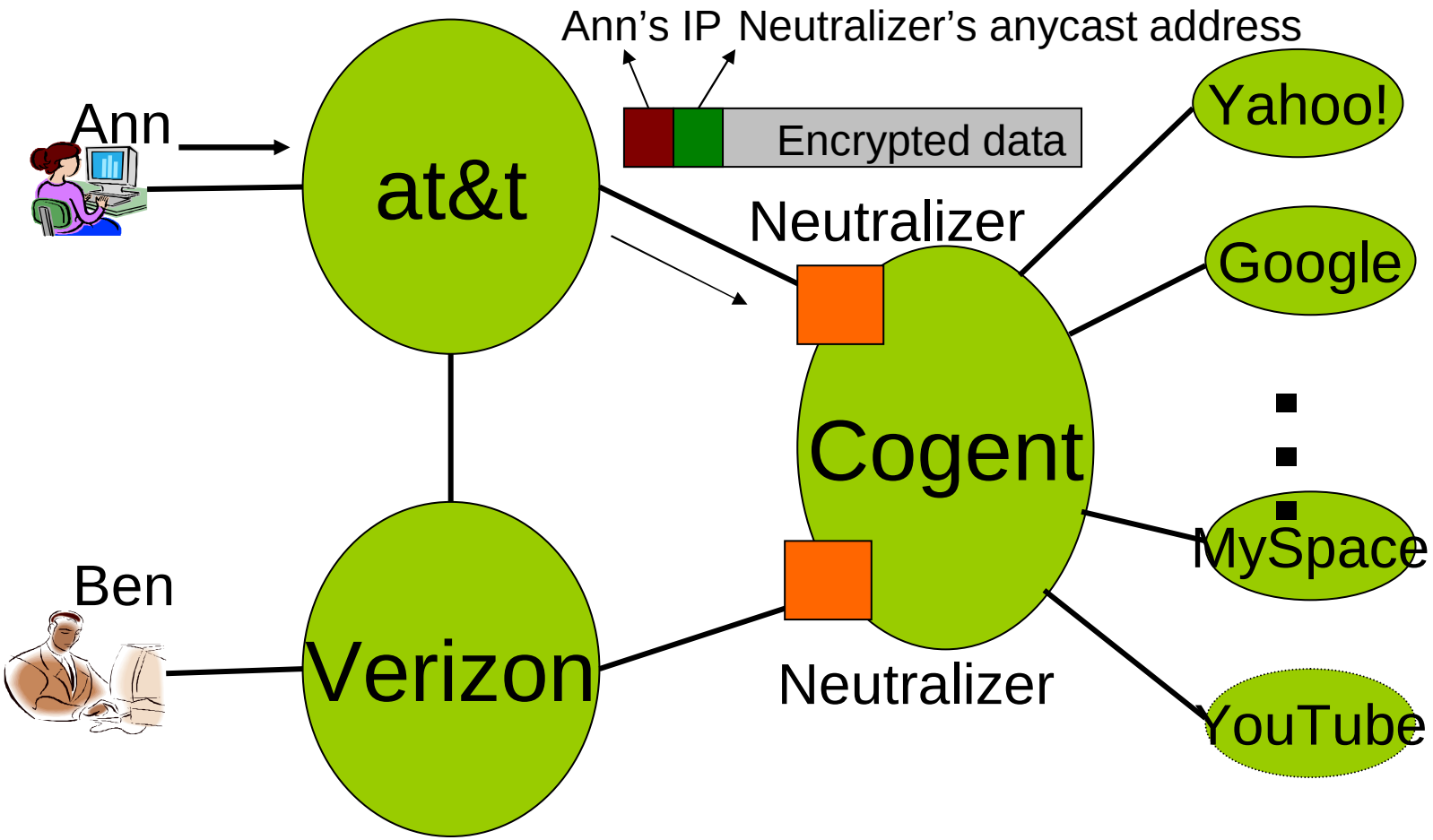
- Assumption: it's too risky to discriminate all

The Challenges

- ☺ Encryption seals contents
- ☹ Discriminate based on non-customer IP addresses

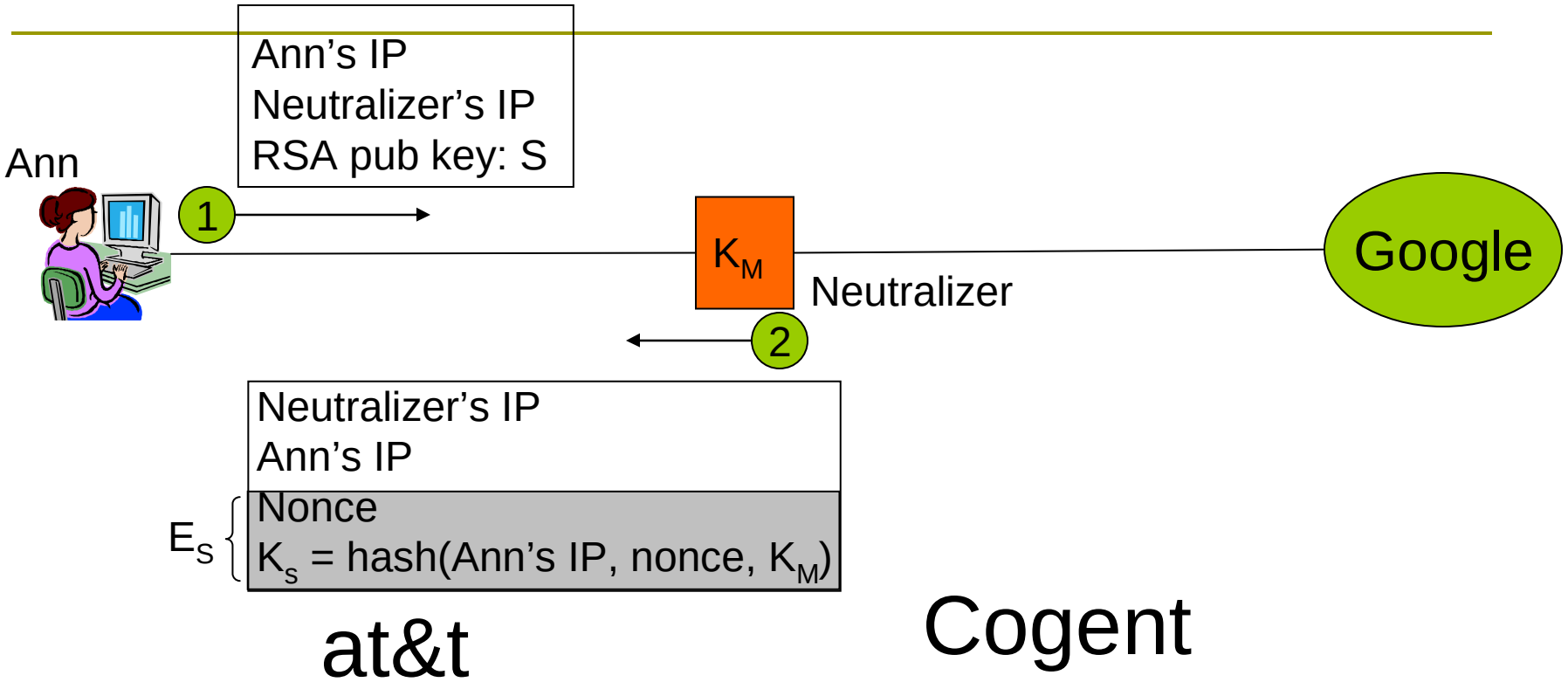
- ☹ Traffic analysis:
  - Discriminate based on inferred application types
  - Not discussed in this paper
    - Less dangerous
    - Harder to be effective
    - Could be alleviated

The big picture



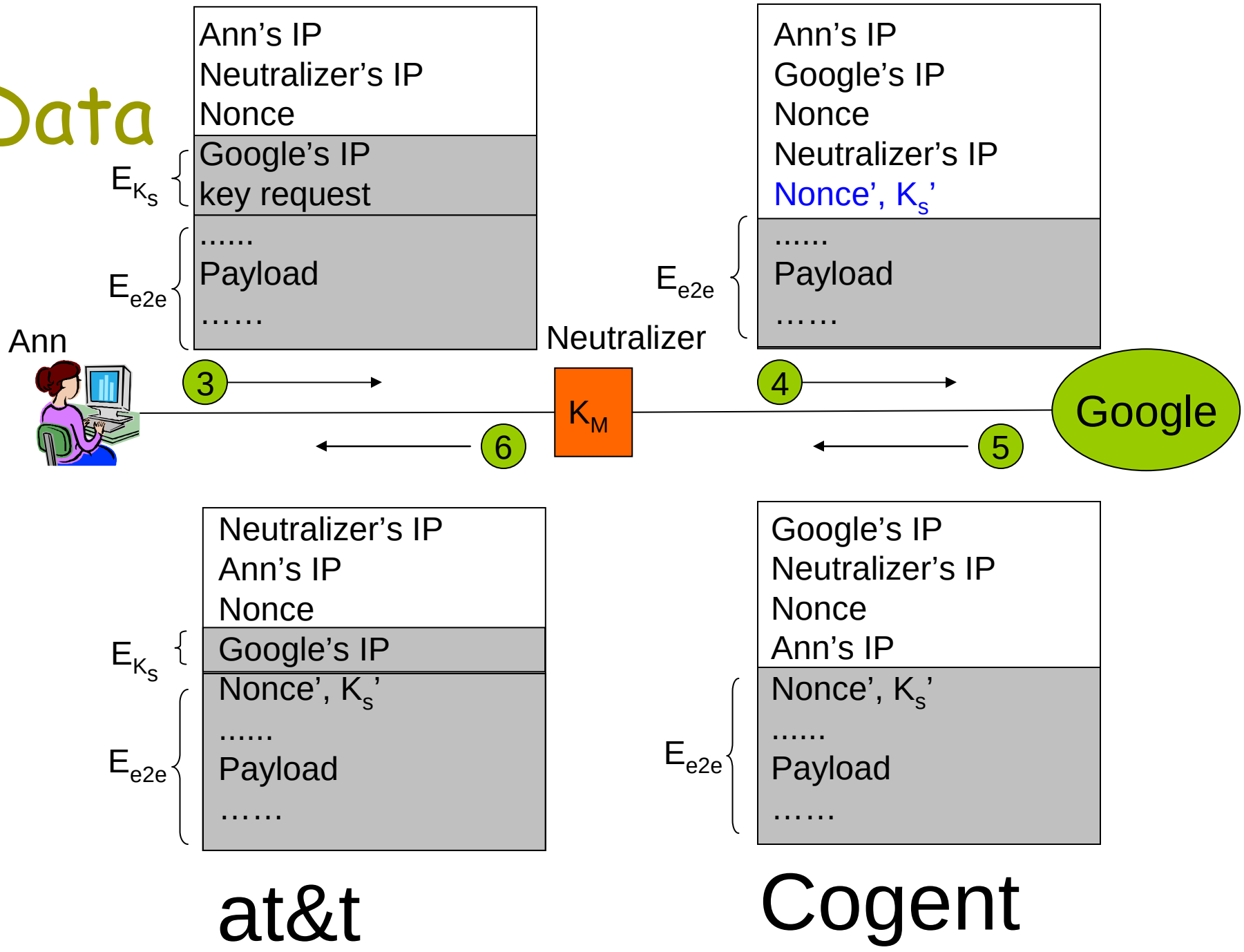
- Requirements: efficiency and robustness

Stateless Key setup

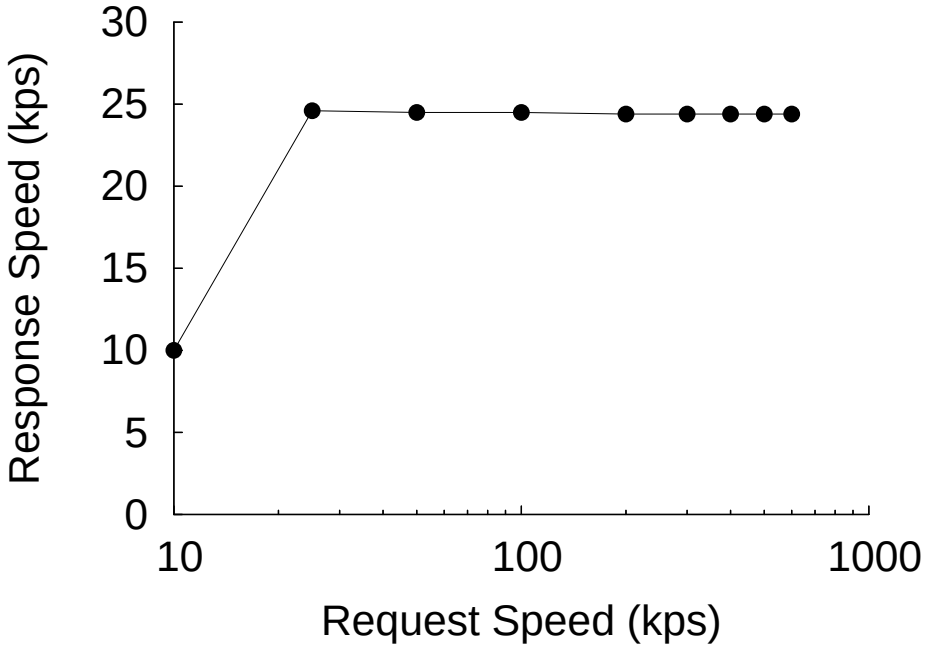


- Efficiency
  - More efficient RSA encryption
  - Offload to a customer
  - Assume no MIM attack
- Robustness
  - Stateless

Data

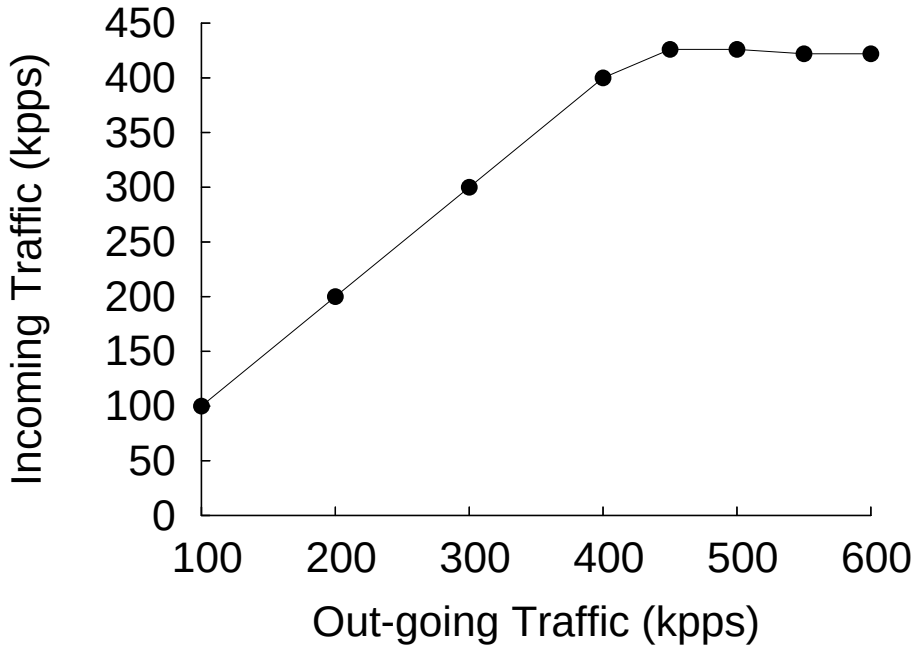

Ann's IP
Neutralizer's IP
Nonce
Google's IP
key request
E_{K_s}
.....
Payload
……
E_{e2e}
Ann
Neutralizer
Ann's IP
Google's IP
Nonce
Neutralizer's IP
Nonce', K_s'
E_{e2e}
.....
Payload
……
3
4
K_M
Google
6
5
Neutralizer's IP
Ann's IP
Nonce
Google's IP
E_{K_s}
Nonce', K_s'
.....
Payload
……
E_{e2e}
Google's IP
Neutralizer's IP
Nonce
Ann's IP
Nonce', K_s'
.....
Payload
……
E_{e2e}
at&t
Cogent

Preliminary Evaluation: key request



- A prototype implementation using Click
- An AMD Opteron 2.6GHz dual core CPU with an Intel pro/1000 GT quad-port server adapter
- 64 bytes UDP packet with 48 bytes header
- 512-bit RSA, and 128-bit AES for encryption

Preliminary Evaluation: data



- Vanilla IP forwarding: 600kpps

Related work

- Anonymous routing
  - Onion Routing, ToR
  - Slicing the onion
- Our work
  - Connectionless
  - IP-layer anonymization

Conclusion

- A technical alternative to keep the net neutral: a clean QoS interface such that data prioritization cannot be done based on contents, application types, or non-customer ends of data
- Key idea is to blur all packets
- An efficient and stateless neutralizer to prevent discrimination based on non-customer IP addresses
- Comments are welcome!

What may still go wrong?

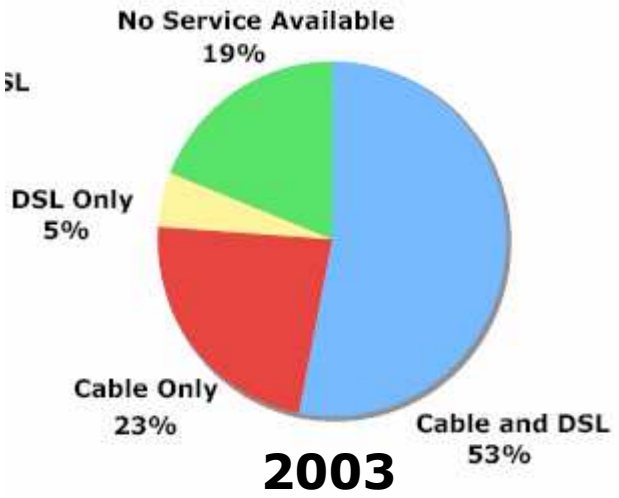
- ISPs can still discriminate
  - Based on customers' or neutralizers' addresses
  - All neutralized or encrypted traffic
  - Key setup packets

  But we prevent deterministic discrimination based on data ownership

- No more good-intentioned data filtering
  - A price we have to pay

- DoS attacks on neutralizers
  - Leveraging existing mechanisms

Why is it a problem now?



2003

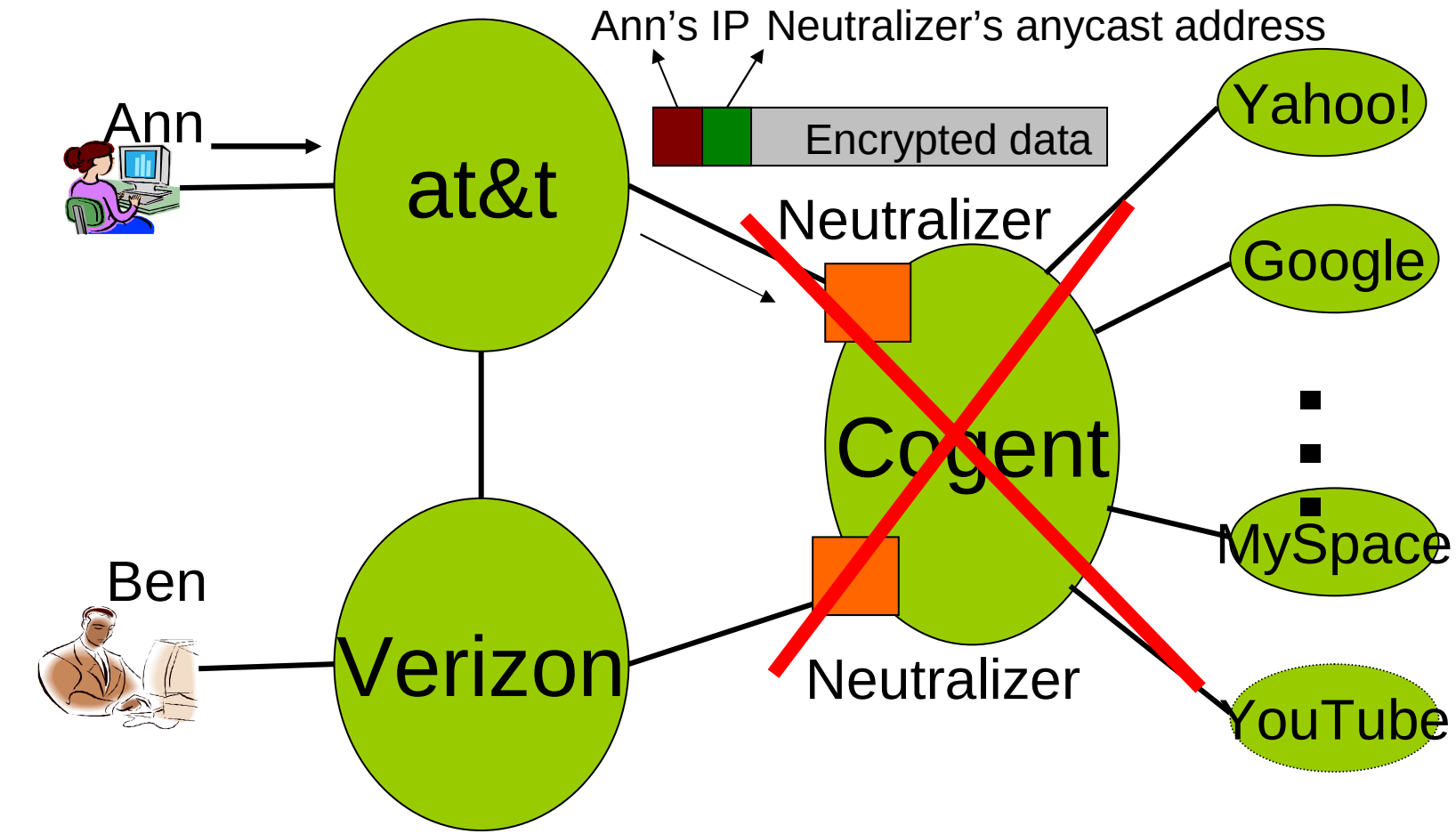
Incumbent Cable and DSL have 99.5 percent of all broadband consumers.

2005

Source: FCC

- Both DSL and Cable are non common carriers
  - In August 2005, DSL was classified as an information service.
  - In March 2002, Cable was classified as an information service.
    - The Brand X case in June 2005
- Lack of facility-based competition

An additional remark



- Prevent local ISPs from exporting market power to the wide area market → NIRA

Other nuisances

- UCI Campus network
  - Planet lab experiments blocked
    - Too many ssh connections in a short interval
  - Desktop computer blocked during upgrade
    - UDP queries sent by NTP exceed threshold
  - No p2p applications on the wireless network
- Hotel Internet connection does not work
  TCP_window_scaling option blocked