FuDiCo III
June 4th, 2007

Rational behavior in large networks of ISP-owned devices

Fabio Picconi Ozalp Babaoglu

University of Bologna, Italy

1

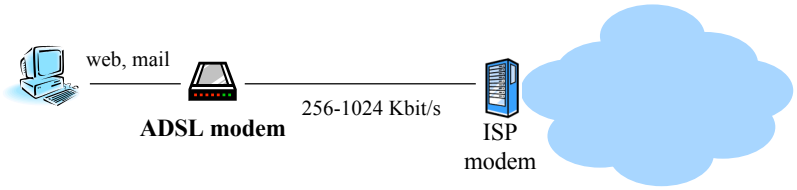
Outline

- **networks of ISP-owned devices**
- **issues related to rational behavior**
  - single-ISP networks
  - multiple-ISP networks
- **conclusions**

2

Evolution of residential Internet access

Typical scenario five years ago:

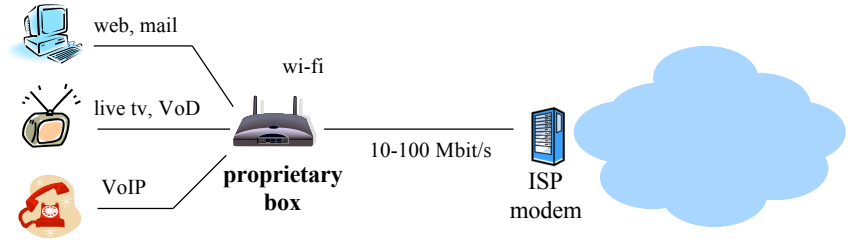


- standard ADSL modem
- modem often purchased by user
- low bandwidth (< 1 Mbit/s)
- applications run on PC
- connection inactive when PC is turned off

3

Evolution of residential Internet access

Typical scenario today:



- proprietary ISP box
- box leased to the user
- high bandwidth (ADSL: 10 MBit/s, FTTH: 100 MBit/s)
- services running on ISP boxes (streaming, VoIP, wi-fi gateway)
- box always on and connected to the network

4

ISP boxes are becoming full-blown computers

Hardware

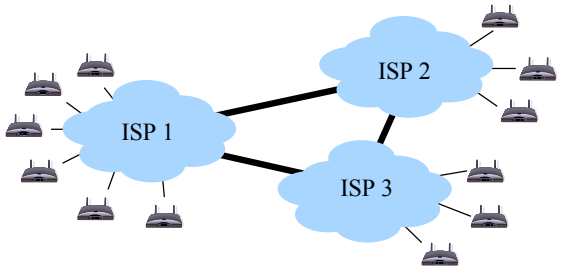
- 300 MHz CPU
- 128 MB RAM
- 40 GB internal hard disk
- Ethernet, wi-fi
- USB, PCMCIA ports

Software

- Linux-based OS
- Media center software
- FTP server

5

Networks of ISP-owned devices



- ISP are deploying a large number of boxes
  - large amount of hardware resources (CPU, storage, bandwidth)
- box OS and services are managed by the ISP
  - controlled execution environment, low churn rate

ideal platform to deploy large-scale P2P services

6

An alternative to cluster and server-based solutions

Devices may be used by ISP for:

- server-less e-mail
- distributed backup
- video-on-demand repositories
- P2P streaming
- distributing computing

many services may be hidden from the user

7

Challenges

Network of a single ISP

- monitoring
- management
- fault-tolerance
- security
- tampered boxes

Federation of multiple ISPs

- protocol compatibility
- high latency
- low bandwidth
- enforcement of SLAs or collaboration between ISPs
- opaqueness

8

Tampered ISP boxes

Motivated users may hack their boxes to:

- gain partial or full control of the box
- remove bandwidth caps
- access internal hard disk capacity
- avoid contribution of local hardware resources
  - storage: free up hard disk for personal use
  - streaming: do not upload to other nodes to free up bandwidth

although rare, tampered boxes are a financial loss for the ISP who pays for the box hardware

9

Tampered ISP boxes

Difficulties in detecting deviant behavior

- distinguishing between selfishness and other causes
  - older hardware revisions → contribute fewer resources (storage, CPU, bandwidth)
  - congestion → drop packets, service fewer requests
- detection may be expensive
  - large-scale monitoring
  - cross-checking of device hardware revision, resource allocation, network state

10

Tampered ISP boxes

Possible solutions to detect/prevent deviant behavior

- Detect: code attestation
  - hardware-based: requires Trusted Platform Module (TPM), increasing costs
  - software-based: Pioneer [SOSP'05], ineffective when firmware is replaced
- Prevent: BAR-tolerant protocol (BAR-B, BAR gossip)
  - too strong: assumes **all** nodes may deviate for personal benefit
  - our scenario: most nodes follow the official protocol
  - does not enforce participation

11

Tampered ISP boxes

Questions:

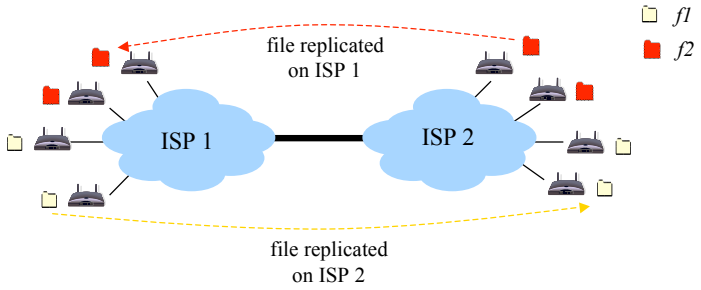
- can infrequent deviant behaviors be detected reliably without incurring substantial costs in every node?
- would such mechanism be cheaper than hardware security?

12

ISP federations

ISP may collaborate to increase aggregate capacity

- spread load peaks over higher number of nodes
- larger number of CPUs for parallel computing applications
- replicate data on other ISPs to increase availability and durability



13

ISP federations

Problem: nodes may be configured (by ISP) to behave

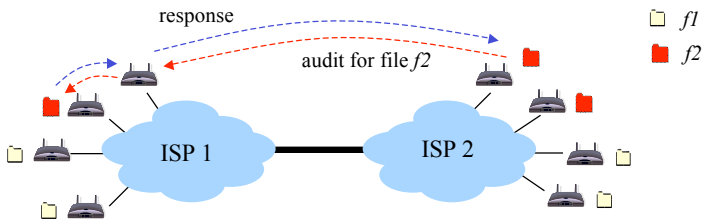
- altruistically with nodes within same ISP
  - follow standard protocol
- selfishly with nodes from other ISPs
  - erase object replicas
  - avoid seeding streams
  - delay processing requests

14

ISP federations

Difficulties in detecting deviant behavior

- opaqueness
  - ISP internal state invisible to other ISPs
- collusion among same-ISP nodes
  - inter-ISP audits may be ineffective



15

ISP federations

Applying existing BAR-tolerant protocols

- replicated state machine (BAR-B)
  - too expensive for inter-ISP communications
  - the *witness node* abstraction requires RSMs
- pairwise exchange (BAR gossip)
  - relies on *broadcaster* node to gather evidence of misbehavior
  - broadcaster node may ignore evidence of nodes within same ISP

16

ISP federations

Questions:

- what mechanisms are necessary to reliably audit an ISP from another one?
- can the witness node abstraction be implemented with low overhead in a multiple-ISP environment?

17

Conclusions

- ISPs currently deploying sophisticated, remotely-controlled devices
- great potential for large-scale cooperative P2P services
- possibility of deviant behavior if devices are tampered with
  - hacked devices cause financial loss to ISP
  - tampering will be rare, lightweight detection mechanism needed
- selfish behavior may arise in multi-ISP networks
  - detection is difficult due to opaqueness and collusion within ISP
  - RSM-based solutions too expensive, audits may not be effective
- question: can a low-overhead, protocol-based solution be found?

18