Rational behavior in large networks of ISP-owned devices

Fabio Picconi, Ozalp Babaoglu
University of Bologna, Italy
{picconi,babaoglu}@cs.unibo.it

Abstract

Internet Service Providers (ISPs) are replacing traditional residential modems with much more sophisticated set-top boxes, thus creating huge networks of ISP-owned embedded computers. This scenario will clearly enable ISPs to run large-scale cooperative services over these networks. However, such systems may exhibit uncooperative behavior either due to tampered devices, or due to devices belonging to different providers. In this paper we outline some of the issues that need to be considered when designing the infrastructure and services so as to exploit the huge economic potential that is possible in such systems.

1 Introduction

Residential Internet access has changed dramatically in the last few years. ADSL speeds exceeding 10 MBit/s are now commonplace, and "Fiber to the home" is growing rapidly. However, we are observing another fundamental change in this area. Instead of shipping simple modems, ISPs are placing increasingly sophisticated devices at the user premises. These set-top boxes are actually small embedded computers equipped with multimedia and wireless connectivity, running an ISP-controlled operating system (usually linux) plus a series of services such as VoIP, video streaming, FTP servers, etc. Recent devices even include an internal hard disk for persistent massive storage.

An important point is that these devices are usually not the property of the user, but are provided by the ISP as part of a lease contract. Also, the devices typically remain under full control of the provider, who manages them remotely to add new services, perform firmware upgrades, etc. User control is usually limited to plugging/unplugging the device, and possibly installing expansions (e.g., video decoders, additional wireless interfaces).

In other words, ISPs are currently setting up extremely large networks of inexpensive, fully-controlled computers directly connected to their networks and to the Internet. Clearly, these networks will open up new possibilities for ISPs to run large-scale peer-to-peer applications in a controlled manner. Thus, these networks are expected to provide stronger service guarantees than open peer-to-peer systems such as current file sharing networks. For instance, the churn rate will be much lower than in current p2p networks, as users normally keep their modem boxes continuosly powered and connected to the network. Also, ISPs may decide to allocate a portion of the device resources to run applications hidden to the user. Thus, the devices could be used by ISPs to offer a low-cost alternative to centralized architectures for commercial services such as content distribution, backup, parallel computing, etc.

Of course, there are several technical challenges to be adressed before such networks can be deployed. One of them is detecting and tolerating devices that do not behave according to their specifications. This includes faulty devices, but also devices tampered by subscribers wishing to gain partial or full control of them, for instance, to remove bandwidth caps, or to have access to the device's internal hard disk. Such users may also install modified firmwares that implement a selfish behavior [4], for instance, by refusing to seed multimedia streams or rejecting requests to store other users' files on the device's hard disk. Clearly, the system should be designed to prevent, or at least detect, such deviant behaviors.

A different form of selfish behavior may arise if several providers decide to federate their devices, e.g., to achieve a higher aggregate capacity or to distribute load peaks across a larger number of nodes. However, a provider may decide to configure its devices to act altruistically with devices within its own network, but selfishly with those belonging to other providers. For instance, it may configure a streaming application to only seed to devices within its own network. If contractual obligations force ISPs to cooperate with each other, the system should support reliable "Proofs of Misbehavior" (POMs) [1] to deter ISPs from uncooperative behaviors.

In the following section we briefly discuss some of the issues that must be taken into account when designing mechanisms to handle selfish behavior in networks of ISP-owned devices.

2 Enforcing cooperation

2.1 Single ISP

Providers must detect tampered devices that do not contribute their resources to the rest of the network. These devices represent a financial loss for the ISP, who has payed for hardware that does not provide any return benefits. Thus, the actual objective is not to prevent tampering, but to avoid non-cooperation. In fact, a tampered device that is forced to cooperate can be an acceptable solution if this is less expensive than preventing tampering.

One way to verify that a remote platform is running untampered software is to use code attestation [3]. However, hardware-based attestation requires including a tamper-proof chip in every decice, thus increasing costs. Software-based solutions exist, but they are not effective when the attacker replaces the platform's firmware.

The BAR model [1, 2] is effective in enforcing cooperation, but it is too strong for our scenario. BAR-tolerant protocols assume that all nodes are selfish, and thus employ techniques that produce significant overhead. Conversely, selfish devices are expected to be rare in our case. Clearly, a more lightweight solution should be employed.

Device heterogeneity and variable load conditions may render detection of tampered devices difficult. For instance, a hacked firmware could continue running ISP-controlled services, but allocate fewer resources to them, disguising as a slower or overloaded device. Also, whenever possible, tampered devices may simply choose not to participate in protocols that enforce collaboration, allocating their resource elsewhere. These behaviors could be detected by monitoring each device's activity, and cross-check it with the device's hardware specification, resource assignment, and the current state of the ISP network, but this mechanism could also produce a significant overhead.

2.2 Federated ISPs

In this scenario an ISP may configure its nodes to act selfishly with respect to nodes belonging to other ISPs. This behavior is similar to that of the BAR model, the main difference being that devices behave altruistically with nodes belonging to their "home" network.

Although BAR-tolerant protocols could be used to ensure cooperation, this solution can be very expensive in network terms. For instance, the BAR-B backup application [1] uses a replicated state machine (RSM) with 3-phase commits for each operation. This is acceptable for LAN environments, but is too expensive for nodes spanning several ISPs. Also, RSMs do not scale well, usually being limited to dozens of nodes.

Another problem is that nodes within an ISP may collude to prevent other ISPs from detecting deviant behavior. For instance, if a device receives an audit request from another ISP, it could forward the request to another node within its network who can provide a valid response to the audit. For example, it would be difficult for an ISP to check that a file is replicated more than once on another ISP's devices.

Similarly, the nodes of an ISP may collude to construct false evidence, for example, that a node replied to a request from another ISP when in fact it did not. In other words, a mechanism must be found to implement reliable *witness nodes* in a collusion-resistant manner.

An interesting question is whether witness nodes and audits can be implemented reliably while minimizing inter-ISP communications. Ideally, audits would be carried from within the same network, and the results propagated to other networks only when necessary (e.g., when a cheating or colluding node is discovered). However, it is unclear whether this can be achieved or not.

3 Conclusions

We have discussed several issues related to selfishness in large networks of ISP-owned, remotely-located computing devices. This scenario differs from the BAR model in that only a small subset of nodes may behave selfishly. Nevertheless, selfish behavior produces a financial loss for the network owner, and therefore should be avoided.

Selfishness may also arise in federations of such networks, as each provider may avoid cooperation when possible. The main difficulty in this case lies in enforcing cooperation while minimizing inter-ISP traffic and resisting intra-ISP collusion.

References

[1] A. Aiyer, L. Alvisi, A. Clement, M. Dahlin, J-P. Martin, C. Porth. BAR Fault Tolerance for Cooperative Services. In *Proc. of SOSP*, 2005.

[2] H. Li, A. Clement, E. Wong, J. Napper, I. Roy, L. Alvisi, M. Dahlin. BAR Gossip. In *Proc. of OSDI*, 2006.

[3] A. Seshadri, M. Luk, E. Shi, A. Perrig, L. van Doorn, and P. Khosla. Pioneer: Verifying Integrity and Guaranteeing Execution of Code on Legacy Platforms. In *Proc. of SOSP*, 2005.

[4] S. Nielson, S. Crosby, D. Wallach. A Taxonomy of Rational Attacks. In *Proc. of IPTPS*, 2005.