

On Designing Resource Sharing Peer-to-Peer Systems

Tsuen-Wan “Johnny” Ngan

Dan S. Wallach*

Department of Computer Science, Rice University

Conventional computer security research usually focuses on the protection of a computer platform. The usual goal is to design systems such that agents (users or programs) will only be able to perform certain actions that are deemed “legitimate” by the system administrators. For example, fair usage on a file server can be enforced by the server owner by employing, say, quota systems. However, such a simplistic approach is not applicable to peer-to-peer (p2p) systems. First, nodes in p2p systems are distributed in nature, making it hard to enforce any policy. Second, there is usually no centralized authority to own and oversee everything. Third, nodes in open p2p systems can have arbitrary, unpredictable behaviors.

These problems are in fact quite similar to the field of *mechanism design*, or sometimes known as *inverse game theory*, in the economics literature. In this model, agents are assumed to act rationally. In other words, it is entirely possible that agents would act selfishly to benefit themselves at others’ expense. The goal of the system designer is thus to design a *strategyproof* mechanism, where agents, acting selfishly, would still maximize the overall utility. As such, economic incentives have to be designed directly into the system so that it would be in the best interest of the agents to follow the rules. Under such mechanisms, the system would be predictable and stable, as all (selfish) agents would follow the rules, and no agent could increase their utility by unidirectionally changing their strategy.

Other than to be strategyproof, we also list some important assumptions for designing a mechanism for an open resource sharing p2p system:

- **Distributed over centralized.** P2p systems are designed to scale. Centralization prevents scalability. Eliminating centralization also avoids central point of failure and vulnerability.
- **Avoid gossiping.** Nodes might lie about their peers. Thus, any reliance on gossip might allow false information to spread throughout the network. You can only really trust what you observe directly about your peers.
- **Be robust against collusion.** Likewise, be wary about trusting a group of nodes. As in real life, collusion and even bribery could occur as a result of agents contending for scarce resources. As such, every node should have a large number of peers with which it regularly communicates to ensure it always has legitimate peers.
- **The need for altruism.** Without a reliable accounting or payment system, there is no way to guarantee that services provided to others will be paid back. If no one services anyone without receiving prior service, no one would start providing service. To bootstrap the service, nodes have to speculatively give free service and hope to get free service in return. In BitTorrent [1], for instance, despite employing a “tit-for-tat” strategy, nodes also allocate a limited amount of their bandwidth for altruistic service. Of course, the downside is that the altruism could be exploited by freeloaders to only receive services.

We have designed mechanisms for both storage and bandwidth sharing in p2p systems. Storage fairness is enforced by requiring nodes to publish their storage records and allowing auditing to those records [2]. Bandwidth fairness is enforced by having nodes locally track the amount of data transferred and limiting each node’s interactions to a small number of nodes that are proven trustworthy [3]. Thus, a node must provide good service to receive good service.

References

- [1] B. Cohen. Incentives build robustness in BitTorrent. In *Workshop on Economics of Peer-to-Peer Systems*, Berkeley, CA, June 2003.
- [2] T.-W. J. Ngan, D. S. Wallach, and P. Druschel. Enforcing fair sharing of peer-to-peer resources. In *2nd International Workshop on Peer-to-Peer Systems (IPTPS’03)*, Berkeley, CA, Feb. 2003.
- [3] T.-W. J. Ngan, Animesh Nandi, and Atul Singh. Fair bandwidth and storage sharing in peer-to-peer networks. In *First IRIS Student Workshop*, Cambridge, MA, Aug. 2003.

*Email: {twngan,dwallach}@cs.rice.edu