

Towards a Dependable, Heterogeneity-Aware P2P System

Tsuen-Wan “Johnny” Ngan Atul Singh Peter Druschel Dan S. Wallach*
Department of Computer Science, Rice University

Peer-to-Peer (P2P) networks are usually designed to be homogeneous, where each node has equal functionality and responsibility. This design is inefficient, since the resources available on high capacity nodes could remain unused, while low capacity nodes become bottlenecks, limiting the performance of the networks. Several techniques have been used to incorporate heterogeneity into P2P systems. These techniques allow resource-rich participants to step up and provide disproportionate amount of resources. They work efficiently and effectively in cooperative environments.

Ideally, every node in a P2P network should honestly contribute its resources to benefit everyone. However, in open environments like the Internet, nodes may be selfish and refuse to contribute their resources. Moreover, malicious nodes will lie about their resource contribution to attack the network. If properly launched, attacks on these techniques can jeopardize the dependability and reliability of the whole networks, with possible attacks range from low-level routing attacks like intercepting and modifying traffic to high-level application-specific attacks like censoring documents, redistributing resources, or any other mischief. Before we can integrate such techniques into open P2P systems, we need to first resolve the following problems:

- **Rational users tend not to provide resources.** In open P2P systems, one cannot force high capacity participants to contribute extra resources. Users are generally self-interested and have no natural incentives to provide their resources if they cannot benefit from doing so. Without such incentives, the only nodes that freely contribute more resources are those that are either ignorant or wish to attack the network.
- **Attackers may lie on resource contribution.** Normally, resource contributions of a node cannot be easily and reliably measured. Practical systems typically allows each node to declare its own level of contributions. An attacker can always claim to possess high capacity. By claiming to provide more resources, attackers can seize more control and exert more power to the network.
- **Attackers may provide poor services.** Even if an attacker is forced to provide services to the network, it can still provide the services as promised at a very low quality. For example, in a search application, an attacker can always return “*Not Found*” instead of the correct results.

To this end, we suggest that the following design primitives should be used to more securely incorporate heterogeneity into open P2P networks.

- **Incentives.** We can induce more competition in resource provision by attracting more correct nodes to provide their resources. This can be done by designing incentives directly into the P2P applications, such that it is in rational users’ best interest to cooperate and provide their resources to the network.
- **Accountability.** Users that promised to provide certain resources should be held accountable. Resource commitments should be enforceable in such a way that users must provide such resources, or risk getting punished and/or evicted from the system.
- **Service evaluation.** It is equally important to measure the *quality of service* each peer is providing. A node that consistently provides poor service should be avoided. In this way, correct nodes can get around malicious nodes that always provide poor services.

At the moment, we are looking into the appropriateness of applying these principles to existing applications. We are also considering whether these principles are complete (i.e., both necessary and sufficient). This work is a continuation of our research on P2P systems and economic incentives, a collaboration of the Pastry project [1] and Rice Computer Security Lab [2].

References

- [1] The Pastry project. <http://freepastry.rice.edu/>.
[2] Computer Security Lab: Rice University. <http://seclab.cs.rice.edu/>.

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