**CSC2231 – Internet Systems and Services**

**Paper Review – Serving DNS using P2P lookup**
**Name: Alex Wun**
**Date: Nov. 9th, 05**

The authors propose a DNS scheme implemented on top of Chord that takes DNSSEC into consideration. A resource record set consists of a domain name and all its mappings. Each resource set is signed by a public key that is obtained by issuing a DNS query for the key (domain name to key mapping). This mapping is in turn signed by the parent domain in the hierarchy and so on up to the root domain.

Implementing DNS over Chord allows the service to inherit scalability and fault-tolerance from the overlay architecture. This design avoids the need for dedicated root DNS servers that currently serve a disproportionately large amount of traffic (largely due to incorrectly setup name servers). Also, by automatically providing routing and fault-tolerance, DNS becomes much easier for administrators to use – hence, fewer incorrect configurations that lead to useless DNS traffic.

Unfortunately, Chord itself suffers from certain deficiencies. It is only fault-tolerant to a certain degree since the routing tables need to be constantly maintained in order for the hashing lookups to function correctly. Chord is also suffers from potential partitioning problems as mentioned by the authors. The most severe flaw (which leads the authors to conclude that this scheme is not feasible) is that lookups in Chord have a much higher lookup cost. Performance is an order of magnitude slower in the median case. However, the variability of lookup costs is much less when compared to traditional DNS. So this architecture manages to avoid the worst case in DNS lookups. If the average lookup cost can be brought closer to costs of traditional DNS lookups, then this would clearly be a better solution in terms of service quality. Some form of proactive replication would likely ease performance problems.