CSC2231 – Internet Systems and Services

Paper Review – Secure Routing
Name: Alex Wun
Date: Nov. 16th, 05

The authors of this paper present an overview of various techniques used to establish secure routing in overlay networks. The three problems they address are: secure assignment of node IDs, secure maintenance of routing tables, and reliable forwarding of messages (high probability delivery). More specifically, an attacker must not be allowed to choose his own IDs since most of a structured P2P's behaviour depends on node IDs. Routing tables must remain correct enough (contain enough non-malicious entries) to route successfully to correct nodes. And dropped or diverted messages must be detected and retransmitted to the intended recipients,

Many of the solutions presented are based on some form of "over compensation". For instance, they propose intentionally slowing down the rate at which nodes can obtain IDs and maintaining a constrained routing table in addition to the regular routing table – which are functional, but inelegant solutions. There also seems to be a general recognition that secure routing is a difficult problem and that no good solution currently exists. Some of the proposals are weak: deferring to a centralized authority to assign certified IDs that become less useful when frequent IP changes are taken into consideration. Or proposing that an increasingly prohibitive cost be incurred for requesting node IDs – a solution that seems to be more of business plan than anything else.

It is also unclear what exactly the *secure routing primitive* is – it is motivated in the paper but never concisely summarized or mentioned in the conclusion. As such, it is unclear how well they contributed to solving the secure P2P routing problem.