Towards Attack-Tolerant Networks: Multipath Fault Tolerance

Edward L. Platt[1] and Daniel M. Romero[1]

1. University of Michigan, Ann Arbor, MI, USA

Networks with single points of failure are particularly susceptible to targeted attacks. In communication networks, these types of faults can leave users vulnerable to censorship and targeted surveillance, even when cryptography is utilized. Centralized networks have single points of failure by definition, leading to a growing popularity in decentralized architectures and protocols. However, centralized network structure can arise even when protocols are decentralized. Despite being based on decentralized protocols, the Internet and World-Wide Web have been shown both theoretically and historically to be highly susceptible to adversarial faults [1], in part due to emergent structural centralization. Existing network trust models, such as webs of trust [2], fail to adequately address network structure. We describe a novel, adversarial fault-tolerant, concurrent multipath routing algorithm for the decentralized butterfly network topology [3]. We also develop a partial trust model that makes it possible to quantify the adversarial fault tolerance of a network, and which makes more realistic transitivity assumptions than webs of trust. When network topology can be dictated, these results can be used to create scalable, attack-tolerant infrastructures. More generally, our results provide a formalism for evaluating the effects of network structure on adversarial fault tolerance.

[1] R. Albert et al. Error and attack tolerance of complex networks. *Nature,* 406(6794), 2000.
[2] P. R. Zimmermann. *The Official PGP User's Guide.* MIT Press, 1995.
[3] A. D. Kshemkalyani and M. Singhal. *Distributed Computing: Principles, Algorithms, and Systems*. Cambridge University Press, 2008.

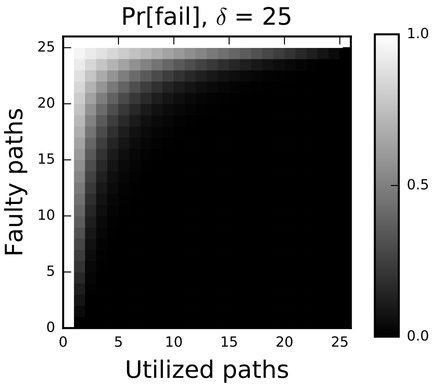

Figure 1: In multipath fault tolerance, the failure probability decreases rapidly with the number of message copies, and increases slowly with the number of faults. Messages are difficult to attack and easy to defend.