Towards Attack-Tolerant Networks: Multipath Fault Tolerance

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

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

Centralized systems are susceptible to targeted attacks against central points, suggesting the importance of decentralization in attack-tolerant systems. While many techniques exist for tolerating random faults, better techniques for tolerating *adversarial faults* such as targeted attacks are needed. In communication networks, targeted attack can leave users vulnerable to censorship and surveillance of messages at central points. Even when encryption is used, it can be bypassed by coercion, e.g., subpoenas. While decentralized *protocols* have become a popular approach to attack-tolerance, centralized network *structure* can arise even when protocols are decentralized. Despite their 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. In this work, we present 1. A fault tolerace scheme for networked communication having a failure probability that decreses exponentially with the number of available independent paths; 2. A routing algorithm for constructing such indpendent paths in the butterfly network topology [2]; and 3. A bounded-transitivity trust model that makes it possible to quantify the adversarial fault tolerance of a network. Our work is the first theoretical demonstration of a point-to-point communication network architecture able to tolerate coercion and other targeted attacks, without requiring infinitely transitive trust. We also evaluate the fault tolerance of an imperfectly implemented butterfly topology by partially rewiring a snapshot of the internet's router network. We find that rewiring only 10% of the edges allows the network to withstand faults in the most central 2% of nodes, increasing to 8% of nodes for 90% rewiring. Our results show that it is possible, in principle, to create highly attack-tolerant communication systems that can withstand targeted and coercive attacks, but only when it is possible to influence network structure.

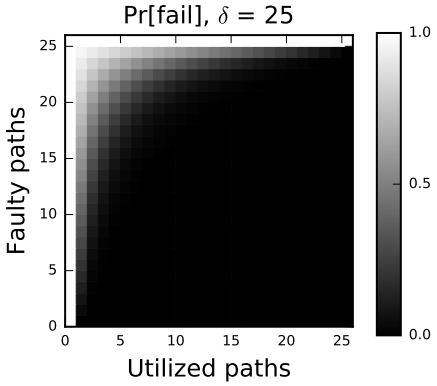

Figure 1: Failure probability decreases rapidly with the number of message copies, and increases slowly with the number of faults. Messages are difficult to attack and easy to defend.

[1] R. Albert et al. Error and attack tolerance of complex networks. *Nature,* 406(6794), 2000.
[2] A. D. Kshemkalyani and M. Singhal. *Distributed Computing*. Cambridge U. Press, 2008.