Improving The Resiliency Of Indirection-Based DDoS Protection Mechanisms Using Per-Packet Path Diversity

Angelos Stavrou
Computer Science Dept.
Columbia University
angel@cs.columbia.edu

Angelos D. Keromytis
Computer Science Dept.
Columbia University
angelos@cs.columbia.edu

Indirection-based overlay networks have recently been proposed as a promising approach for countering distributed denial of service (DDoS) attacks. Such mechanisms are based on the assumption that attackers cannot eavesdrop on specific links inside the network and thus gain information that can assist them in focusing their attacks. This assumption is perhaps one of the key limitations of these systems, and we identify several scenarios and environments where such attacks are possible.

To address this issue, we propose to use a spread-spectrum-like paradigm to create per-packet path diversity. Briefly, we exploit the natural diversity of paths available between any host and the various overlay nodes to spread the traffic. We describe how to achieve this without sacrificing the strong authentication requirements of such architectures or allowing an attacker with partial information to repeatedly disrupt communications. Surprisingly, our approach also allows us to detect attackers that have subverted one or more overlay nodes and are using them to launch a DDoS attack. We use our prototype implementation on PlanetLab, a distributed testbed for experimentation with overlays, to determine the end-to-end latency and sustainable throughput for communications using our scheme.