Mitigating Denial-of-Service Attacks on the Chord Overlay Network: A Location Hiding Approach

Serverless distributed computing has received significant attention from both the industry and the research community. Among the most popular applications are the wide-area network file systems, exemplified by CFS, Farsite, and OceanStore. These file systems store files on a large collection of untrusted nodes that form an overlay network. They use cryptographic techniques to maintain file confidentiality and integrity from malicious nodes. Unfortunately, cryptographic techniques cannot protect a file holder from a denial-of-service (DoS) attack or a host compromise attack. Hence, most of these distributed file systems are vulnerable to targeted file attacks, wherein an adversary attempts to attack a small (chosen) set of files by attacking the nodes that host them. The present Location Guard is a location hiding Technique for securing overlay file storage systems from targeted file attacks Location Guard has essential components: 1) location key, consisting of a random bit string (e.g., 128 bits) that serves as the key to the location of a file, 2) routing guard, a secure algorithm that protects accesses to a file in the overlay network given its location key such that neither its key nor its location is revealed to an adversary.