Mitigating Denial-of-Service Attacks in Contested Network Environments

Abstract

In an increasingly connected world, ensuring availability of the services and applications carried by computer networks is critical. As the most far-reaching computer network, the Internet is the home to millions of services that have profound influences on people's life and work. Additionally, mobile ad hoc networks (MANETs), often used to support critical military and civilian projects, rely on the availability of all participating nodes to fulfill their missions. However, the availability of these networks and services are constantly threatened by denial-of-service (DoS) attacks with growing intensity and sophistication. In this thesis, we study different DoS combating mechanisms to protect services and hosts in the contested Internet and MANET environments.

To mitigate distributed denial-of-service (DDoS) attacks bombarded by powerful botnets on the Internet, we propose a moving target mechanism that progressively separates benign clients from the mingled attackers. This is achieved by endowing mobility to the defense system to evade naive attackers, and smartly shuffling clients to quarantine advanced attackers. We present two mobile defense architectures tailored for different threat and application models. One architecture, named MOTAG, is built on secret moving network proxies that act as the intermediate layer between authenticated clients and the protected services. By only disclosing the active proxies to the authenticated clients and quickly replacing the attacked ones, this intermediate layer becomes a moving target that continues to escape from network flooding attacks. Another architecture, enabled by the resource elasticity and network space of cloud computing, replicates open web servers to partition incoming clients' workload. By dynamically instantiating new replica servers scattered in the cloud and re-shuffling clients' assignments, we are able to quarantine flooding attacks targeting both network and computational resources. Under both architectures, advanced attackers may follow the moving targets to persist their attacks. To isolate the following attackers from benign clients, we perform elaborate shuffling operations that intelligently redistribute clients among different proxies or replica servers. For guiding the shuffling operations, we design an optimal dynamic programming algorithm that expectedly saves the maximum number of benign clients from each shuffle. We also introduce a much faster greedy algorithm that can generate near-optimal shuffling plans in realtime. Furthermore, a maximum-likelihood algorithm is employed to accurately estimate the number of following attackers. Results from extensive simulations show that our defense mechanism can save a vast majority of benign clients from persistent and intense DDoS attacks in a few rounds of shuffling. Experiments that study the overhead of the shuffling operation demonstrate that clients can be re-assigned among different proxies or replica servers in several seconds.

In addition, this thesis introduces a capability-based mechanism that inhibits MANET DoS attacks in the context of multi-path routing. Existing solutions are limited because they assume a single path is used to route traffic for each flow. To prevent attacks that multiply their throughput by employing multiple different routes, we present CapMan, an enhanced capability-based mechanism that enforces per-flow limits across all employed routes. To ensure overall capability compliance, CapMan not only informs all intermediate nodes of a flow about the assigned capability, but also provides them with a global throughput perspective via periodical summary exchange. Results show that CapMan is able to maintain flow-wide capability constraints consistently and distributedly, even when multiple colluding insiders attempt to exacerbate the attack. In the meantime, the impact of CapMan on well-behaved flows is shown to be small.