A Control-Theoretic Framework for Dynamic Quarantine in DDoS Defense

Shane C. Baccas

May 5, 2025

1 Introduction

We propose a novel control-theoretic approach to mitigating Distributed Denial-of-Service (DDoS) attacks through a dynamic quarantine actuator. Unlike traditional static thresholds or heuristic filtering, our method models the defense system as a feedback controller that regulates quarantining based on traffic volatility and system stress.

2 System Overview

Let $\lambda(t)$ denote the observed incoming traffic rate (e.g., packets per second), and $\sigma(t)$ be the sample standard deviation of traffic measured over a rolling window. Define a trigger threshold based on a multiplier s such that:

$$\lambda(t) > \mu + s \cdot \sigma(t) \quad \Rightarrow \quad \text{Activate quarantine actuator} \tag{1}$$

Let $q(t) \in [0, 1]$ be the fraction of traffic quarantined at time t. Then:

$$\lambda_q(t) = q(t) \cdot \lambda(t) \tag{2}$$

$$\lambda_s(t) = (1 - q(t)) \cdot \lambda(t) \tag{3}$$

where λ_q is inspected, and λ_s is served normally.

3 State Variables and Dynamics

We define the system state vector as:

$$x(t) = \begin{bmatrix} \lambda(t) \\ \sigma(t) \\ b(t) \\ \ell(t) \end{bmatrix} \tag{4}$$

where:

- $b(t)$: buffer utilization or server backlog
- $\ell(t)$: response latency

State evolution is governed by:

$$\dot{b}(t) = \lambda_s(t) - C_{\text{proc}} \tag{5}$$

$$\dot{\ell}(t) = \kappa \cdot b(t) \tag{6}$$

Here, C_{proc} is the processing capacity of the server, and κ maps backlog to latency.

4 Control Inputs

The control input is:

$$u(t) = \begin{bmatrix} q(t) \\ s(t) \end{bmatrix} \tag{7}$$

The controller chooses $q(t)$ and $s(t)$ to manage load, minimize damage, and control cost.

5 Detection Function

The effectiveness of filtering quarantined traffic is modeled as:

$$D(q, \lambda_q) = \frac{1}{1 + e^{-\beta(q \cdot \lambda - \theta)}} \tag{8}$$

where β is the detection sensitivity and θ is a learned threshold.

6 Cost Functions

Defender Cost

$$J_D = \int_0^T \left[\alpha q(t)\lambda(t) + C_S \lambda_s(t) + \gamma \ell(t)\right] dt \tag{9}$$

Attacker Cost

$$J_A = \int_0^T c_a \cdot \lambda_a(t)\, dt \tag{10}$$

where $\lambda_a(t)$ is attacker-generated traffic.

7 Objective

The defender seeks to minimize J_D over a time horizon $[0, T]$, subject to dynamics:

$$\dot{x}(t) = f(x(t), u(t))$$
$$x(t) \in \mathcal{X}, \quad u(t) \in \mathcal{U}$$

This yields a constrained optimal control problem that balances cost, latency, and inspection aggressiveness in the presence of adversarial traffic.