

Mathematical Models for Network Anomaly Detection

Making Sense of Chaos using Statistics and Probability

Computer Networks Project

January 23, 2026

The Core Problem: Signal vs. Noise

Imagine a busy hospital hallway.

- **Normal Busy:** Doctors, nurses, and patients moving with purpose. It's crowded, but efficient.
- **Attack (DDoS):** A thousand people suddenly running down the hall screaming the same word.

How do we teach a computer to tell the difference?

1. Shannon Entropy (Measuring Surprise)

Concept: Entropy measures *uncertainty*.

The Coin Toss Analogy

- **High Entropy:** A fair coin. 50% Heads, 50% Tails.
- **Low Entropy:** A rigged coin. 100% Heads. Zero surprise.

Entropy in Networks

$$H(X) = - \sum P(x_i) \log_2 P(x_i)$$

- **Normal Traffic:** Mix of types (HTTP, VoIP, DICOM).
High Entropy (≈ 3.0)
- **DDoS Attack:** Flood of ONE type (UDP).
Low Entropy ($\rightarrow 0.0$)

2. EWMA (Smoothing the Jitter)

Exponentially Weighted Moving Average

$$RTT_{new} = (1 - \alpha) \cdot RTT_{old} + \alpha \cdot RTT_{current}$$

- Latency jumps around a lot.
- We use a "memory" factor (α) to smooth the curve.
- Ignores brief spikes, catches real congestion.

3. Z-Score (Spotting Outliers)

$$Z = \frac{Value - Average}{StandardDeviation}$$

- **Z = 0**: Average behavior.
- **Z > 3: Extremely Rare!** (Anomaly)

Used to detect Flash Crowds (massive volume spikes).

4. Congestion Severity Score (CSS)

$$CSS = 0.5 \cdot Latency + 20.0 \cdot Loss + 2.0 \cdot (1 - Entropy)$$

- Combines Latency, Packet Loss, and Entropy.
- **Score 1**: Healthy
- **Score 4**: **CRITICAL ALERT**

Summary

Algorithm	Purpose
Shannon Entropy	Detect Attacks
EWMA	Smooth Latency
Z-Score	Detect Outliers
CSS	Combined Decision